

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2001年 5月31日

出 願 番 号
Application Number: 特願2001-165580

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

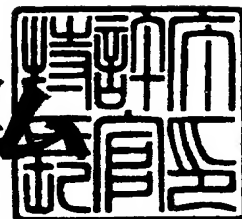
J P 2001-165580

出 願 人
Applicant(s): トレンドマイクロ株式会社

2009年10月15日

特許庁長官
Commissioner,
Japan Patent Office

細野 哲子



【書類名】 特許願

【整理番号】 TM-01

【提出日】 平成13年 5月31日

【あて先】 特許庁長官 殿

【国際特許分類】

G06F 13/00

H04L 9/00

H04L 12/28

H04L 12/46

H04L 12/66

【発明の名称】 データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

【請求項の数】 28

【発明者】

【住所又は居所】 アール．オー．シー，台湾，台北，チュン フォア，エス．アールディー．エスイーシー．2，319，9階 トレンドマイクロ インコーポレイテッド

【氏名】 リー，フランク

【特許出願人】

【識別番号】 397011166

【氏名又は名称】 トレンドマイクロ株式会社

【代理人】

【識別番号】 100098084

【弁理士】

【氏名又は名称】 川▲崎▼ 研二

【選任した代理人】

【識別番号】 100111763

【弁理士】

【氏名又は名称】 松本 隆

【手数料の表示】

【予納台帳番号】 038265

【納付金額】 21,000

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

【特許請求の範囲】

【請求項 1】 データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信し、当該データの宛先へ送信するステップと、

前記サーバが、前記送信したデータに応答して前記宛先から送信されてくる応答データを受信するステップと、

前記サーバが、前記宛先から受信した応答データに対してセキュリティチェックを行うステップと、

前記サーバが、前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信するステップと

を備えることを特徴とするデータ通信方法。

【請求項 2】 データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信するステップと、

前記サーバが、前記受信したデータに対してセキュリティチェックを行うステップと、

前記サーバが前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するステップと

を備えることを特徴とするデータ通信方法。

【請求項 3】 請求項 1 又は 2 に記載のデータ通信方法において、

前記情報通信装置は、プロバイダが提供するインターネット接続サービスを受けることにより、インターネットを介してデータを送受信する装置であり、

前記プロバイダの通信装置が、前記情報通信装置のユーザが前記サーバによって行われるセキュリティチェックを受けるための契約情報を当該情報通信装置から受信するステップと、

前記プロバイダの通信装置が、前記受信した契約情報を前記サーバに転送するステップと、

前記サーバが、前記サーバから転送されてくる契約情報を受信し、記憶するステップと

を備え、

前記セキュリティチェックを行うステップにおいて、前記サーバは前記記憶している契約情報に基づいて前記セキュリティチェックを行う

ことを特徴とするデータ通信方法。

【請求項4】 請求項3に記載のデータ通信方法において、

前記プロバイダの通信装置が、前記受信した契約情報に基づいて、前記データ中継装置においてデータ転送の要否を判断するための情報を当該データ中継装置に転送するステップと、

前記データ中継装置が、前記プロバイダの通信装置から転送されてくる情報を受信し、記憶するステップと

を備え、

前記データ中継装置が転送するステップにおいて、前記データ中継装置は前記記憶している情報に基づいて前記転送の要否を判断して前記転送を行う

ことを特徴とするデータ通信方法。

【請求項5】 請求項1又は2に記載のデータ通信方法において、

前記情報通信装置は、プロバイダが提供するインターネット接続サービスを受けることにより、インターネットを介してデータを送受信する装置であり、

前記プロバイダの通信装置が、前記サーバによって行われるセキュリティチェックの内容に応じて、前記情報通信装置のユーザに課金するための処理を行うステップを備えることを特徴とするデータ通信方法。

【請求項6】 データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバと

からなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、

前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、

前記受信したデータを当該データの宛先へ送信するデータ送信手段と、

前記送信したデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信する応答データ送信手段と

を備えることを特徴とするデータ通信システム。

【請求項 7】 データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバとからなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、

前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えることを特徴とするデータ通信システム。

【請求項 8】 データの送受信を行って当該データの伝送を中継する通信手段と、

前記通信手段によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信手段を用いて転送する転送手段

と

を備えることを特徴とするデータ中継装置。

【請求項 9】 請求項 8 に記載のデータ中継装置において、
前記転送手段によって前記受信データを前記サーバへ転送する必要があるか否かを判断する判断手段を備え、

前記転送手段は、前記判断手段によって転送要と判断された場合に前記受信データを前記サーバへ転送することを特徴とするデータ中継装置。

【請求項 10】 請求項 9 に記載のデータ中継装置において、
前記判断手段は、前記受信データの送信元が前記サーバでない場合に転送要と判断することを特徴とするデータ中継装置。

【請求項 11】 請求項 10 に記載のデータ中継装置において、
外部の通信装置から送信されてくる前記サーバの通信アドレスを受信するアドレス受信手段と、

前記受信した通信アドレスを記憶するアドレス記憶手段と
を備え、

前記判断手段は、前記受信データに含まれている当該受信データの送信元の通信アドレスと、前記アドレス記憶手段に記憶されている通信アドレスとに基づいて前記転送の要否を判断することを特徴とするデータ中継装置。

【請求項 12】 請求項 9 に記載のデータ中継装置において、
前記判断手段は、
前記受信データが従うプロトコルに基づいて転送の要否を判断するための要否判断情報を記憶する要否判断情報記憶手段と、

前記受信データに含まれているプロトコル識別情報と、前記要否判断情報記憶手段に記憶されている要否判断情報とに基づいて前記転送の要否を決定する決定手段と

を備えることを特徴とするデータ中継装置。

【請求項 13】 請求項 12 に記載のデータ中継装置において、
外部の通信装置から送信されてくる前記要否判断情報を受信する要否判断情報受信手段を備え、

前記要否判断情報記憶手段は、前記受信した要否判断情報を記憶することを特徴とするデータ中継装置。

【請求項 14】 データの送受信を行って当該データの伝送を中継する通信手段と、

自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するための装置識別情報を記憶する記憶手段と、

前記通信手段によって受信された受信データに対して前記記憶手段に記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信手段を用いて転送する転送手段と

を備えることを特徴とするデータ中継装置。

【請求項 15】 請求項 14 に記載のデータ中継装置において、

前記装置識別情報は前記データ中継装置のシリアルナンバーであり、

前記転送手段は、前記転送先へ転送する受信データにおけるトランスポート層プロトコルのペイロードに前記シリアルナンバーを書き込んで当該受信データを転送することを特徴とするデータ中継装置。

【請求項 16】 請求項 8～15 のいずれか 1 に記載のデータ中継装置において、

前記データ中継装置は、ネットワーク層プロトコルに従ってルーティングを行うルータであることを特徴とするデータ中継装置。

【請求項 17】 データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータを当該データの宛先へ送信するデータ送信手段と、

前記データ送信手段によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信する応答データ送信手段と

を備えることを特徴とするサーバ。

【請求項 18】 請求項 17 に記載のサーバにおいて、
前記セキュリティチェックを行う対象となる応答データは、前記情報通信装置宛のコンテンツであることを特徴とするサーバ。

【請求項 19】 請求項 17 に記載のサーバにおいて、
前記セキュリティチェックを行う対象となる応答データは、前記情報通信装置宛の電子メールであることを特徴とするサーバ。

【請求項 20】 データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えることを特徴とするサーバ。

【請求項 21】 請求項 20 に記載のサーバにおいて、
前記セキュリティチェックを行う対象となるデータは、前記情報通信装置が送信した電子メールであることを特徴とするサーバ。

【請求項 22】 請求項 17 又は 20 に記載のサーバにおいて、
正当な前記データ中継装置に割り当てられた識別情報を記憶する記憶手段を参照し、当該記憶手段に記憶されている識別情報と、前記データに付加されて転送されてくる当該データの転送元のデータ中継装置の識別情報とを照合することにより、前記転送元のデータ中継装置の正当性を確認する認証手段を備えることを特徴とするサーバ。

【請求項 23】 請求項 22 に記載のサーバにおいて、
前記識別情報は前記データ中継装置のシリアルナンバーであり、
前記データに付加されるシリアルナンバーは、当該データにおけるトランスポート層プロトコルのペイロードに書き込まれており、
前記認証手段は、前記データにおけるトランスポート層プロトコルのペイロードに書き込まれたシリアルナンバーを読み出して前記正当性の確認を行うことを特徴とするサーバ。

【請求項 24】 コンピュータに、
データの送受信を行って当該データの伝送を中継する通信機能と、
前記通信機能によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信機能を用いて転送する転送機能と
と
を実行させるためのプログラム。

【請求項 25】 コンピュータに、
データの送受信を行って当該データの伝送を中継する通信機能と、
自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するための装置識別情報を記憶する記憶機能と、
前記通信機能によって受信された受信データに対して前記記憶機能によって記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信機能を用いて転送する転送機能と
を実行させるためのプログラム。

【請求項 26】 コンピュータに、
データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、
前記受信したデータを当該データの宛先へ送信するデータ送信機能と、
前記データ送信機能によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信機能と、
前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック機能と、
前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信する応答データ送信機能と
を実行させるためのプログラム。

【請求項 27】 コンピュータに、
データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、
前記受信したデータに対してセキュリティチェックを行うセキュリティチェッ

ク機能と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信する
データ送信機能と

を実行させるためのプログラム。

【請求項 28】 請求項 24～27 のいずれか 1 に記載のプログラムを記録
したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、インターネット等のコンピュータネットワークにおいて、様々な不正行為による被害を防止するためのデータ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体に関する。

【0002】

【従来の技術】

インターネットはオープンなネットワーク環境であるがゆえに、世界規模で急速に普及してきた。しかし、その一方で、いわゆるコンピュータウィルスやジャンクメール等の不正行為による被害が数多く発生している。

そこで、これらの問題に対する対抗策が従来から各種提案されている。例えばコンピュータウィルスに対してはワクチンソフトと呼ばれる対抗策が採られている。このワクチンソフトは、コンピュータの外部から進入してきたコンピュータウィルスを検出してこれを駆除するためのコンピュータプログラムであり、ユーザのパソコンにインストールして利用される。

【0003】

【発明が解決しようとする課題】

コンピュータウィルスの検出技術の代表的なものとして、例えばパターンマッチング方式がある。これは既知のコンピュータウィルスのコードの中からこのウィルスに固有のコードパターンを「ウィルス定義ファイル」と呼ばれるファイルに記憶しておき、このウィルス定義ファイル内のコードパターンと検索対象のファイルのコードとを比較してコンピュータウィルスの存在を検出するというもの

である。

【０００４】

このパターンマッチング方式は、より迅速にコンピュータウィルスを検出できるという点で優れているが、新たなコンピュータウィルスが出現する度にこれを１つ１つ解析してコードパターンを抽出するという事前処理が必要となるため、新種のコンピュータウィルスに対しては対応が遅れてしまうという問題がある。

そこで、ワクチンソフトの提供者は、最新のコンピュータウィルスに対応したウィルス定義ファイルを自身のホームページ上に用意しておき、ユーザはこのホームページにアクセスして自身のワクチンソフトをアップデートする等して、この問題に対処している。しかし、ユーザからみれば、このようなアップデート作業は非常に煩わしいものである。

【０００５】

また、ジャンクメールについても、既知のジャンクメールの類型パターンを記憶しておき、これと照合してジャンクメールを検出するというような対応策が考えられる。しかし、これも上記コンピュータウィルスと同様の問題が生じてしまう。

【０００６】

本発明は、このような背景の下になされたものであり、ユーザの利便性を損ねることなく、インターネット等のコンピュータネットワークにおいて様々な不正行為による被害を防止するためのデータ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体に関する。

【０００７】

【課題を解決するための手段】

上述した課題を解決するため、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信し、当該データの宛先へ送信するステップと、

前記サーバが、前記送信したデータに応答して前記宛先から送信されてくる応

答データを受信するステップと、

前記サーバが、前記宛先から受信した応答データに対してセキュリティチェックを行うステップと、

前記サーバが、前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信するステップと

を備えるデータ通信方法を提供する。

この方法によれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに回答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【0008】

また、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信するステップと、

前記サーバが、前記受信したデータに対してセキュリティチェックを行うステップと、

前記サーバが前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するステップと

を備えるデータ通信方法を提供する。

この方法によれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うことができる。

【0009】

また、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバとからなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、
前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、
前記受信したデータを当該データの宛先へ送信するデータ送信手段と、
前記送信したデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信する応答データ送信手段と

を備えるデータ通信システムを提供する。

このシステムによれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【0010】

また、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバとからなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、

前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えるデータ通信システムを提供する。

このシステムによれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うことができる。

【0011】

また、本発明は、データの送受信を行って当該データの伝送を中継する通信手段と、

前記通信手段によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信手段を用いて転送する転送手段と

を備えるデータ中継装置を提供する。

この装置によれば、セキュリティチェックを行うサーバへ受信データを転送先へ転送することができる。

【0012】

また、本発明は、データの送受信を行って当該データの伝送を中継する通信手段と、

自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するための装置識別情報を記憶する記憶手段を備え、

前記通信手段によって受信された受信データに対して前記記憶手段に記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信手段を用いて転送する転送手段と

を備えるデータ中継装置を提供する。

この装置によれば、受信データに装置識別情報を付加して予め定められた転送先へ転送することができる。

【0013】

また、本発明は、データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータを当該データの宛先へ送信するデータ送信手段と、

前記データ送信手段によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信

する応答データ送信手段と

を備えるサーバを提供する。

このサーバによれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【0014】

また、本発明は、データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えるサーバを提供する。

このサーバによれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うことができる。

【0015】

また、本発明は、コンピュータに、

データの送受信を行って当該データの伝送を中継する通信機能と、

前記通信機能によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信機能を用いて転送する転送機能と

を実行させるためのプログラムを提供する。

このプログラムによれば、セキュリティチェックを行うサーバへ受信データを転送することができる。

【0016】

また、本発明は、コンピュータに、

データの送受信を行って当該データの伝送を中継する通信機能と、

自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するため

の装置識別情報を記憶する記憶機能と、

前記通信機能によって受信された受信データに対して前記記憶機能によって記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信機能を用いて転送する転送機能と
を実行させるためのプログラムを提供する。

このプログラムによれば、受信データに対して装置識別情報を付加し、この装置識別情報が付加された受信データを予め定められた転送先へ転送することができる。

【0017】

また、本発明は、コンピュータに、

データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、

前記受信したデータを当該データの宛先へ送信するデータ送信機能と、

前記データ送信機能によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信機能と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック機能と、

前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信する応答データ送信機能と

を実行させるためのプログラムを提供する。。

このプログラムによれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【0018】

また、本発明は、コンピュータに、

データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェッ

ク機能と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信する
データ送信機能と

を実行させるためのプログラムを提供する。

このプログラムによれば、データ中継装置によって転送されてくるデータを受
信すると、受信したデータに対してセキュリティチェックを行うことができる。

【0019】

【発明の実施の形態】

以下、図面を参照して、この発明の実施形態について説明する。ただし、本発
明は、かかる実施形態に限定されず、その技術思想の範囲内で種々の変更が可能
である。

【0020】

A：構成

まず、実施形態の構成について説明する。

(1) システムの全体構成

図1は、実施形態に係るシステムの全体構成を示すブロック図である。図1に
示すように、このシステムは、ホームネットワーク1、ADSL (Asymmetric
Digital Subscriber Line) 網2、インターネットサービスプロバイダ (以下
ISPと略称) 3、インターネット4、センタ5及びWWWサーバ6を備えてい
る。なお、図1においては、システム構成を簡単に説明するために、ホームネッ
トワーク1、ISP3及びWWWサーバ6をそれぞれ1つしか図示していないが
、実際にはこれらの構成要素はそれぞれ複数存在している。

【0021】

ホームネットワーク1は、ユーザの家庭に設置されたローカルエリアネットワ
ークである。このホームネットワーク1は、各種の情報通信装置10～13、ル
ータ14、ADSLモデム15、及びこれらを接続する各種通信ケーブルを備え
ている。図1では情報通信装置の一例として、パーソナルコンピュータ (以下P
Cと略称) 10、テレビジョン11、MP3 (MPEG-1 Audio Layer-3) プレー
ヤ12、PDA (Personal Digital Assistants) 13を示しているが、この

他にも例えばデジタルカメラ、ゲーム用機器、セットトップボックス、携帯電話機、冷蔵庫、電子レンジ、防犯システム等の様々な機器を利用することが可能である。これら情報通信装置10～13は、WWW (World Wide Web) ブラウザ等の文書閲覧プログラムを搭載しており、インターネット4に接続された各種サーバが提供する情報を取得し表示することが可能になっている。

【0022】

ルータ14は、ツイストペアケーブル（例えば10BASE-Tケーブル）や同軸ケーブル等の通信ケーブルによって情報通信装置10～13に接続されるとともに、モジュラーケーブル等の通信ケーブルを介してADSLモデム15に接続されている。このルータ14は、自身が記憶しているルーティングテーブルに基づいてデータ伝送を中継する周知のルーティング機能を備える他、所定の条件に基づいて中継対象のデータをセンタ5に転送する転送機能を備えている。

ここで、ルータ14は、上記転送機能を実現する際に、センタ5内に設置されたセキュリティサーバ51（後述する）を情報通信装置10～13の代理となるプロキシサーバに指定し、このセキュリティサーバ51に対していわゆるトンネリングを行ってデータ転送を行うようになっている。

【0023】

ADSLモデム15は、モジュラーケーブル等の通信ケーブルを介してADSL網2に接続されている。このADSLモデム15は、ADSL網2とホームネットワーク1との間でデータ信号の授受が可能となるように、このデータ信号の変復調を行う機能を備えている。

【0024】

センタ5は、図示せぬルータを介してインターネット4に接続されている。このセンタ5は、セキュリティサーバ51、シリアル情報データベース（以下データベースをDBと略称）52、セキュリティ契約情報DB53、及びこれらを相互に接続する高速デジタル回線54を備えている。

【0025】

セキュリティサーバ51は、プロキシ機能とセキュリティチェック機能を備えたサーバである。

プロキシ機能とは、前述したように、ルータ 14 から ADSL 網 2 及びインターネット 4 を介して転送されてくるデータを受信すると、受信したデータを情報通信装置 10～13 の代理としてその宛先に送信し、これに応答してその宛先から送信されてくるデータを受信し、これを情報通信装置 10～13 に送信する機能である。

セキュリティチェック機能とは、パターンマッチング等を行ってコンピュータウィルスやジャンクメールを検出し、検出したコンピュータウィルスを周知のアルゴリズムを用いて駆除したり、ジャンクメールを廃棄したりする機能である。この際用いられるコンピュータウィルスの駆除方法としては、コンピュータウィルスに相当するコードを適当なコードに置き換えたり、コンピュータウィルスに感染したデータファイルを削除したり、そのファイルの拡張子を変更したりする等の方法がある。

さらに、このセキュリティサーバ 51 は、情報通信装置 10～13 のユーザがセキュリティチェックを受ける契約を行うための契約申込画面を示すデータ（以下契約申込画面データと呼ぶ）を記憶しており、情報通信装置 10～13 からのリクエストに応じて、この契約申込画面データを送信する機能を備えている。

【0026】

シリアル情報 DB 52 には、既に製造された全てのルータ 14 のシリアルナンバーと、これらルータ 14 の各々に予め割り当てられている個体パスワードとからなるシリアル情報が格納されている。このシリアル情報は、セキュリティサーバ 51 がルータ 14 の正当性を確認するために利用される。

【0027】

セキュリティ契約情報 DB 53 には、情報通信装置 10～13 のユーザとセンタ 5 の管理者との間で交わされるセキュリティチェックの契約の内容を示すセキュリティ契約情報が格納されている。より具体的には、このセキュリティ契約情報は、各ルータ 14 から転送されてくるデータに対し、どのような種類のセキュリティチェックを行うかということを示す情報である。

【0028】

ISP 3 は、図示せぬルータを介して ADSL 網 2 に接続されるとともに、図

示せぬ別のルータを介してインターネット4に接続されている。このISP3は、図1に示したPOPサーバ31、IMAPサーバ32、SMTPサーバ33、契約代行サーバ34、ユーザ情報DB35、課金情報DB36、及びこれらを接続する高速デジタル回線37のほか、図示せぬゲートウェイサーバやDNS (Domain Name Service) サーバを備えている。

このISP3は、上述したサーバ群やデータベース群が連携して機能することにより、情報通信装置10～13に対し、インターネット4への接続サービスや電子メールの中継サービスを提供する。さらに、ISP3は、情報通信装置10～13のユーザとセンタ5と間で交わされるべきセキュリティチェックの契約に関する処理をセンタ5に代わって行う契約代行機能と、このセキュリティチェックに関する課金処理をセンタ5に代わって行う課金代行機能を備えている。

【0029】

以下、ISP3を構成するサーバ及びデータベースの各々が実現する機能の概略を説明する。

まず、POPサーバ31、IMAPサーバ32及びSMTPサーバ33はそれぞれ周知のサーバである。即ち、POPサーバ31はPOP3 (Post Office Protocol version 3) を用いて情報通信装置10～13宛の電子メール（以下受信メール）をその宛て先に配信するサーバである。IMAPサーバ32はIMAP4 (Internet Message Access Protocol version 4) を用いて情報通信装置10～13宛の受信メールをその宛先に配信するサーバである。SMTPサーバ33は、SMTP (Simple Mail Transfer Protocol) を用いて情報通信装置10～13から送信された電子メール（以下送信メール）をその宛先に対応したSMTPサーバ（図示略）へ転送するサーバである。

【0030】

次に、契約代行サーバ34は、前述したセキュリティチェックの契約代行を行うサーバである。より具体的には、契約代行サーバ34は、情報通信装置10～13から送信されてくるセキュリティ契約情報を受信すると、ユーザ認証を行ってユーザの正当性を確認した後、そのセキュリティ契約情報を本来の契約主体であるセンタ5に転送するとともに、当該セキュリティ契約情報をISP3内の

ユーザ情報DB 3 5に転送するようになっている。

【0031】

ユーザ情報DB 3 5には、ISP 3によるIP接続サービスやメール中継サービスを受けるユーザの属性情報に加え、上述のようにして契約代行サーバ3 5から転送されてくるセキュリティ契約情報が記憶されている。

【0032】

課金情報DB 3 6には、ISP 3によるIP接続サービスやメール中継サービスに対応した課金情報に加えて、センタ5が行うセキュリティチェックに対応した課金情報が記憶されている。この課金情報DB 3 6は、専用線を介して金融機関システム7に接続されている。金融機関システム7は、課金情報DB 3 6に記憶されている課金情報に基づいて、ユーザが指定する銀行口座から課金額を引き落とす処理を行うようになっている。

【0033】

WWWサーバ6は、図示せぬルータを介してインターネット4に接続されている。このWWWサーバ6は、各種コンテンツを示すコンテンツデータをHTML (HyperText Markup Language) 形式やXML (Extensible Markup Language) 形式で記憶しており、インターネット4を介して送信されてくるHTTP (HyperText Transfer Protocol) リクエストに応答して、これらコンテンツデータをHTTPレスポンスとして送信するようになっている。

ここで、コンテンツとは、例えばニュース、電子書籍、オーディオ、ビデオクリップ、ホームページというような、テキスト、音楽、画像の少なくともいずれか1つによって表現される情報を意味する他、ゲームソフトやJava（登録商標）アプレット等の各種コンピュータプログラムをも含む概念である。

【0034】

(2) ルータ14の構成

次に、図2のブロック図を参照しながら、ルータ14の構成について説明する。

図2に示すように、ルータ14は、CPU (Central Processing Unit) 141、ROM (Read Only Memory) 142、RAM (Random Access Memory) 14

3、フラッシュメモリ 144、表示部 145、LAN 通信部 146、WAN 通信部 147、及びこれらを相互に接続するバス 148 を備えている。

ROM 142 には、ルーティング処理を行うためのルーティングプログラム等の制御プログラムの他、各ルータ 14 に固有のシリアルナンバーや、このシリアルナンバーに基づいて生成された個体パスワードが記憶されている。この個体パスワードは、シリアルナンバーを構成する文字列を基に所定のアルゴリズムに従って生成される文字列であり、ルータ 14 の製造時にシリアルナンバーとともに ROM 142 に書き込まれる。

CPU 141 は、ROM 142 から制御プログラムを読み出し、これを実行することによってルータ 14 全体を制御する。RAM 143 は、CPU 141 のワークエリアとして用いられ、例えば CPU 141 によって実行される制御プログラムが展開されたり、制御プログラムの実行時に用いられる各種データが一時的に記憶される。

フラッシュメモリ 144 には、ルーティング先の IP アドレスが記述された周知のルーティングテーブルと、ルータ 14 の IP アドレスと、セキュリティサーバ 51 の IP アドレスと、セキュリティサーバ 51 に転送すべきデータが従うアプリケーション層プロトコルのプロトコル名が記述されたチェック対象プロトコルテーブルが記憶されている。これらフラッシュメモリ 144 に記憶されるもののうち、セキュリティサーバ 51 の IP アドレスと、チェック対象プロトコルテーブルに記述されるデータは、ユーザがセキュリティチェックの契約を締結することにより、契約代行サーバ 34 から ADSL 網 2 を介して通知されて、このフラッシュメモリ 144 に記憶されるようになっている。

表示部 145 は、図示せぬ LED (Light Emitting Diode) や液晶パネル等の表示装置と、これを駆動する駆動ドライバとを備えており、CPU 141 の制御の下で各種の状態や情報を表示するようになっている。

LAN 通信部 146 は、図示せぬ 4 ポートハブを備えている。この 4 ポートハブには、各情報通信装置 10～13 に接続される通信ケーブルの端部が挿入され、これにより、各情報通信装置 10～13 とルータ 14 とが相互に接続されるようになっている。LAN 通信部 146、この 4 ポートハブを介して、情報通信装

置10～13との間でデータ通信を行う。

WAN通信部147は、図示せぬADSLポートを備えている。このADSLポートには、ADSLモデム15に接続される通信ケーブルの端部が挿入され、これにより、ADSLモデム15とルータ14とが接続されるようになっている。WAN通信部147は、このADSLポートを介して、ADSLモデム15との間でデータ通信を行う。

【0035】

ここで、図3のフォーマット図を参照しながら、フラッシュメモリ144に記憶されているチェック対象プロトコルテーブルの構成について説明する。

図3に示すように、チェック対象プロトコルテーブルには、セキュリティチェックの対象となるアプリケーション層プロトコルのプロトコル名と、このアプリケーション層プロトコルに対応する宛先ポート番号とが関連付けて記憶されている。ルータ14のCPU141は、中継すべきパケットのTCPヘッダに含まれている宛先ポート番号が、チェック対象プロトコルテーブルに記憶されている宛先ポート番号と一致した場合には、そのパケットをセキュリティサーバ51に転送する。

一方、中継すべきパケットのTCPヘッダに含まれている宛先ポート番号が、チェック対象プロトコルテーブルに記憶されている宛先ポート番号と一致しない場合には、CPU141は、通常のルーティング処理を行う。即ち、CPU141は、パケットのIPヘッダに書き込まれているIPアドレスと、フラッシュメモリ144内のルーティングテーブルとに従って当該パケットをその宛先へ送信するようになっている。

図3に示す例では、POP3、SMTP、HTTPという3種類のアプリケーション層プロトコルのデータをセキュリティサーバ51に転送するように設定されており、これらアプリケーション層プロトコルに対応する宛先ポート番号はそれぞれ「110」、「25」、「80」であることを意味している。

【0036】

(3) センタ5の構成

次に、センタ5の構成について詳細に説明する。

(3-1) セキュリティサーバ51の構成

まず、図4のブロック図を参照しながら、セキュリティサーバ51の構成について説明する。

図4に示すように、セキュリティサーバ51は、CPU511、ROM512、RAM513、通信部514、ハードディスク装置515、及びこれらを相互に接続するバス516を備えている。

ROM512にはIPL (Initial Program Loader) 等の基本制御を司る制御プログラムが格納されている。CPU511は、このROM512やハードディスク装置515から各種プログラムを読み出し、これを実行する。RAM513は、CPU511のワークエリアとして用いられ、例えばCPU511によって実行されるプログラムが展開されたり、プログラム実行時に用いられる各種データが一時的に記憶される。

通信部514は、インターネット4に接続するための接続インタフェースやモデムを備えており、インターネット4を介して各種の通信装置とデータ通信を行う。

ハードディスク装置515には、図4に示す契約申込画面配信プログラムやセキュリティチェックプログラムの他、情報通信装置10～13のプロキシサーバとして機能するための図示せぬプロキシプログラムが記憶されている。契約申込画面配信プログラムは、前述した契約申込画面データを情報通信装置10～13に配信するためのコンピュータプログラムである。CPU511は、情報通信装置10～13のいずれかからの要求に応じて、この契約申込画面配信プログラムを実行し、要求元の情報通信装置10～13に対して契約申込画面データを送信するようになっている。セキュリティチェックプログラムは、セキュリティサーバ51が情報通信装置10～13の代理として送受信するデータに対してセキュリティチェックを行うためのコンピュータプログラムである。このセキュリティチェックプログラムは、新種のコンピュータウィルス等に対応可能となるように、センタ5の管理者によって随時更新されている。

【0037】

(3-2) シリアル情報DB52の構成

次に、図5のフォーマット図を参照しながら、シリアル情報DB52の構成について説明する。

図5に示すように、シリアル情報DB52には、シリアルナンバーと、このシリアルナンバーに基づいて生成された個体パスワードとが対応付けて記憶されている。図5に示す例では、シリアルナンバー「S000001」に対応する個体パスワードが「a b c 1 2 3」であることを意味している。これらのシリアル情報は、ルータ14の製造工場から通知されることにより、このシリアル情報DB52に格納されるようになっている。

【0038】

(3-3) セキュリティ契約情報DB53の構成

次に、図6のフォーマット図を参照しながら、セキュリティ契約情報DB53の構成について説明する。

図6に示すように、セキュリティ契約情報DB53には、各ルータ14の「シリアルナンバー」に対応して、そのルータ14のユーザが契約によって指定した「セキュリティチェックの内容」が記憶されている。図6に示す例では、シリアルナンバー「S000001」に対応するルータ14に対しては、コンピュータウィルスの駆除を目的とした「ウィルスチェック」と、ジャンクメールの廃棄を目的とした「ジャンクメールチェック」とが「オン」設定されており、これらウィルスチェック及びジャンクメールチェックがなされることを意味している。

さらに、このシリアルナンバー「S000001」に対応するルータ14において、ウィルスチェックのチェック対象プロトコルは、「POP3」、「SMTP」、「HTTP」となっている。これは、情報通信装置10～13がPOP3を用いて受信する受信メールと、情報通信装置10～13がSMTPを用いて送信する送信メールと、WWWサーバ6から情報通信装置10～13に対しHTTPレスポンスとして送信されるコンテンツデータに対してウィルスチェックがなされることを意味している。同様に、ジャンクメールチェックのチェック対象プロトコルは「POP3」となっており、これは、情報通信装置10～13がPOP3を用いて受信する受信メールに対してジャンクメールチェックがなされることを意味している。

これらのセキュリティ契約情報は、契約代行サーバ34から通知されることにより、このセキュリティ契約情報DB53に記憶されるようになっている。

【0039】

(4) ISP3の構成

次に、ISP3内に設置されているユーザ情報DB35及び課金情報DB36の構成について説明する。

(4-1) ユーザ情報DB35の構成

図7は、ユーザ情報DB35に記憶されているユーザ情報の一例を示したフォーマット図である。

図7に示すように、ユーザ情報DB35には、ISP3が各ユーザに割り当てた「ユーザID」と「パスワード」、ユーザが使用するルータ14の「シリアルナンバー」とこれに対応する「個体パスワード」、このルータ14に対応した「セキュリティチェックの内容」の他、「ユーザ名」、「住所」、「生年月日」等のユーザの属性情報が、それぞれ関連付けて記憶されている。

例えば図7に示すユーザID「aaa」に対応するユーザについては、図6で説明したシリアルナンバー「S000001」のルータ14に対応するセキュリティチェックの内容と同一のデータが記憶されている。一方、ユーザID「bbb」が示すユーザについては、セキュリティチェックの内容がブランクになっており、このユーザはセキュリティチェックの契約を行っていないことが示されている。

上記の「シリアルナンバー」、「個体パスワード」及び「セキュリティチェックの内容」は、前述したように、契約代行サーバ34から通知されることにより、このユーザ情報DB35に記憶されるようになっている。

【0040】

(4-2) 課金情報DB36の構成

次に、図8のフォーマット図を参照しながら、課金情報DB36の構成を説明する。

図8に示すように、課金情報DB36には、ISP3のユーザに割り当てられた「ユーザID」に対応して、このユーザに対して課された課金額を引き落とす

ための「銀行口座」、ISP 3が提供した接続サービス及びメール中継サービスに対してユーザが毎月支払うべき「ISP課金額」、センタ5が行ったセキュリティチェックに対してユーザが毎月支払うべき「セキュリティチェック課金額」、およびこれらの課金額を合算した「課金額合計」が記憶されている。例えば、ユーザID「aaa」に対応するユーザに対しては、ISP課金額「5000円」とセキュリティチェック課金額「3000円」とを合算した「8000円」が毎月、課金されることを意味している。

ここで、ウィルスチェックとジャンクメールチェックとでは別々に課金されるようになっており、図8に示す例では、ウィルスチェックに関する課金額は「2000円」であり、ジャンクメールチェックに関する課金額は「1000円」に設定されている。

また、ユーザID「bbb」に対応するユーザは、ISP 3によるサービスのみを受けており、センタ5によるセキュリティチェックを受けていないので、セキュリティチェック課金額はブランクになっている。

このような課金情報は、ISP 3が図示せぬ記憶装置に記憶している当該ISP 3自身のサービス契約情報と、上述したユーザ情報DB 35に記憶されているセキュリティチェックに関する情報とに基づいて生成され、この課金情報DB 36に格納される。

以上が本実施形態の構成である。

【0041】

B：動作

次に、上記構成からなる実施形態の動作について説明する。

前述したように、ルータ14は受信したデータをトンネリングを行ってセキュリティサーバに転送し、これに応じて、セキュリティサーバ51は情報通信装置10～13のプロキシサーバとして機能する。

そこで、具体的な動作例を説明する前に、ルータ14とセキュリティサーバ51がデータを送受信する際に行う基本動作を、送受信されるデータの構造とともに説明しておく。

【0042】

図9は、PC10が、POPサーバ31、IMAPサーバ32、SMTPサーバ33及びWWWサーバ6のいずれかとデータ通信を行う際の仕組みを説明する説明図である。なお、PC10が、POPサーバ31、IMAPサーバ32、SMTPサーバ33及びWWWサーバ6のいずれかとデータ通信を行う際には、送受信の対象となるデータは複数のパケットに分割されて送受信されるが、図9においては簡単に説明するため、これら複数のパケットのうちの1つのパケットのみに着目して説明を行う。

【0043】

図9において、まず、PC10は、POPサーバ31、IMAPサーバ32、SMTPサーバ33、WWWサーバ6のいずれか（以下POPサーバ31を例示して説明する）に対して各種要求を行うためのパケットP1を送信する。このパケットP1は、図10のフォーマット図に示すように、IPヘッダの宛先アドレスフィールドには「POPサーバ31のIPアドレス」が記述され、送信元アドレスフィールドには「PC10のIPアドレス」が記述されている。また、TCPヘッダの宛先ポート番号フィールドには「110」番が記述されている。

【0044】

ルータ14は、パケットP1を受信すると、カプセル化を行ってパケットP2を生成し、これをセキュリティサーバ51に送信する。このパケットP2は、図11のフォーマット図に示すように、パケットP1に対してさらにIPヘッダ、TCPヘッダ及びTCPペイロードが付加されたデータ構造となっている。

付加されたIPヘッダの宛先アドレスフィールドには「セキュリティサーバ51のIPアドレス」が記述され、送信元アドレスフィールドには「ルータ14のIPアドレス」が記述されている。

ここで、本実施形態では、ルータ14及びセキュリティサーバ間はSOCKSプロトコルを用いてトンネリングを行うようになっている。そこで、付加されたTCPヘッダには、SOCKSプロトコルにおいて使用する宛先ポート番号フィールドが設けられており、このフィールドには「1050」番が記述されている。さらに、付加されたTCPペイロードには、トンネル用認証情報フィールドが設けられており、このフィールドにはルータ14のフラッシュメモリ144から

読み出された「シリアルナンバー」が記述されている。

【0045】

セキュリティサーバ51はパケットP2を受信すると、まず、TCPペイロードに含まれるシリアルナンバーがシリアル情報DB52に記憶されているか否かによりルータ14の正当性を確認する。次いで、セキュリティサーバ51は、ルータ14によって付加されたIPヘッダ、TCPヘッダ及びTCPペイロードを取り除いて脱カプセル化を行い、パケットP3を得る。さらに、セキュリティサーバ51は、このパケットP3のIPヘッダの送信元アドレスフィールドに書きこまれている「PC10のIPアドレス」を、「セキュリティサーバ51のIPアドレス」に書き換えて、図12のフォーマット図に示すようなパケットP4を生成し、これをPOPサーバ31に送信する。

【0046】

POPサーバ31はパケットP4を受信すると、これに応答して、PC10宛のデータを含むパケットP5をセキュリティサーバ51に送信する。このパケットP5においては、図13のフォーマット図に示すように、IPヘッダの宛先アドレスフィールドに「セキュリティサーバ51のIPアドレス」が記述され、送信元アドレスフィールドには「POPサーバ31のIPアドレス」が記述されている。また、TCPヘッダの送信元ポート番号フィールドには「110」番が記述されている。

【0047】

セキュリティサーバ51は、パケットP5を受信するとIPヘッダの宛先アドレスフィールドの「セキュリティサーバ51のIPアドレス」を「PC10のIPアドレス」に書き換え、送信元アドレスフィールドの「POPサーバ31のIPアドレス」を「セキュリティサーバ51のIPアドレス」に書き換える。さらに、セキュリティサーバ51は、書き換え後のパケットP5に対してカプセル化を行ってパケットP6を生成し、これをPC10に送信する。

このパケットP6においては、図14のフォーマット図に示すように、カプセル化によって付加されたIPヘッダの宛先アドレスフィールドに「ルータ14のIPアドレス」が記述され、送信元アドレスフィールドには「セキュリティサー

バ51のIPアドレス」が記述されている。また、付加されたTCPヘッダの送信元ポート番号フィールドには「1050」番が記述されている。

【0048】

ルータ14は、パケットP6を受信すると、脱カプセル化を行ってパケットP7を得て、このパケットP7をPC10に送信する。

【0049】

このように、ルータ14とセキュリティサーバ51は、中継すべきパケットに対してカプセル化やIPアドレスの書き換え等を適宜行うことにより、データの中継処理を実行している。

なお、上記の例では、PC10とPOPサーバ31とがデータ通信を行う場合を説明したが、PC10以外の他の情報通信装置11～13がその処理主体であってもPC10と動作は共通である。

【0050】

次に、具体的な動作例について説明する。

本実施形態では、まず、ユーザがセキュリティチェックを受けるための契約を締結し、この契約が締結された後に、各プロトコルに応じたセキュリティチェックが実施されることになる。

そこで、以下では、(1)セキュリティチェックの契約、について説明した後、各プロトコルに応じた動作例として、(2)POP3を用いた受信メールに対するセキュリティチェック、(3)SMTPを用いた送信メールに対するセキュリティチェック、(4)HTTPを用いたコンテンツデータに対するセキュリティチェック、について説明する。

【0051】

(1) セキュリティチェックの契約

まず、図15に示すシーケンスを参照しながら、ユーザがセキュリティチェックの契約を締結する際の動作について説明する。

ユーザは、ルータ14を購入すると、通信ケーブルを用いてルータ14と情報通信装置10～13及びADSLモデム15とを接続する。次いで、ユーザは、ルータ14に対し初期設定を行うべく、PC10等を操作してWWWブラウザを

起動させ、このWWWブラウザによって表示される対話画面を参照しながら所定の操作を行う。これに応じてPC10からルータ14に対して設定通知がなされ、ルータ14は、自身のIPアドレスをフラッシュメモリ144に記憶したり、ルーティングテーブルにルーティング先のIPアドレスを書き込む等の処理を行う。このような初期設定が完了すると、ルータ14は、データをルーティング可能な状態になる。

【0052】

次いで、ユーザは、WWWブラウザによって表示された対話画面の所定フィールド内に、ルータ14の仕様書等に記載されているURL (Uniform Resource Locator) を入力する。PC10はこの入力操作を受け付けると(ステップS1)、GETメソッドを用いたHTTPリクエストを契約申込画面要求としてセキュリティサーバ51に送信する(ステップS2)。この契約申込画面要求には、ユーザによって入力されたURLが含まれており、このURLは契約申込画面データを記憶しているセキュリティサーバ51のリソースを示している。

この契約申込画面要求は、ルータ14のルーティング機能によってADSL網2に送出された後、図示せぬゲートウェイやルータを次々と経由してセキュリティサーバ51によって受信される。

【0053】

セキュリティサーバ51は、上記契約申込画面要求を受信すると、これに応じて契約申込画面配信プログラムを起動する。そして、セキュリティサーバ51は、受信した契約申込画面要求に含まれるURLによって指定されるリソースから契約申込画面データを読み出し、これをHTTPレスポンスとしてPC10に送信する(ステップS3)。

【0054】

PC10は、インターネット4及びADSL網2を介して上記契約申込画面データを受信すると、これを解釈して図示せぬディスプレイ装置に契約申込画面を表示する(ステップS4)。

このとき表示される契約申込画面の一例を図16の模式図に示す。図16に示すように、この契約申込画面には、ユーザが加入しているISP名を入力するた

めのフィールドF 1 と、ルータ 1 4 のシリアルナンバーを入力するためのフィールドF 2 と、個体パスワードを入力するためのフィールドF 3 と、ISP 3 によって割り当てられたユーザIDを入力するためのフィールドF 4 と、ユーザIDに対応したパスワードを入力するためのフィールドF 5 と、所望するセキュリティチェックを選択するためのチェックボックスF 6 ～F 1 2 とが設けられている。また、フィールドF 1 の右方には、プルダウンメニューボックスMBが設けられており、ユーザがこのプルダウンメニューボックスMBをマウスでクリックすると、「A社、B社、C社、・・・」というように各ISP名がプルダウンで列記表示され、ユーザはこの中から自身が加入するISP 3 を選択することができる。さらに、このISP名には、対応するISP 3 が備える契約代行サーバ3 4 のIPアドレスが関連付けられている。

図1 6に示すように、ユーザが各フィールドF 1 ～F 1 2 にデータを入力した後、「送信」と表記されたソフトボタンSBをマウスでクリックすると、PC 1 0はこの操作を受け付ける（ステップS 5）。

次いで、PC 1 0は、ユーザによって入力されたISP名に関連付けられている契約代行サーバ3 4 のIPアドレスを宛先として、ユーザによってフィールドF 1 ～F 1 2 に入力されたデータを含むHTTPリクエストを契約要求として送信する（ステップS 6）。

【0 0 5 5】

ISP 3 の契約代行サーバ3 4 は、上記契約要求を受信すると、まず、受信した契約要求の中からユーザID及びパスワードを抽出し、これらがユーザ情報DB 3 5 に記憶されているものと一致するか否かを判断することにより、ユーザ認証を行う（ステップS 7）。ここでは、契約要求に含まれるユーザID「a a a」及びパスワード「x x x z z z」は、図7に示すユーザ情報DB 3 5 に記憶されたものと一致するので、ユーザは正当であると判断されることになる。

【0 0 5 6】

ステップS 7において正当なユーザであると判断された場合には、契約代行サーバ3 4 は、上記契約要求に含まれるユーザID及びパスワード以外のデータ（即ちセキュリティ契約情報）をユーザ情報DB 3 5 に転送し、このユーザ情報D

B 3 5に格納させる（ステップS 8）。即ち、図7に示すように、ルータ1 4のシリアルナンバー「S 0 0 0 0 0 1」及び個体パスワード「a b c 1 2 3」が格納されるとともに、ウィルスチェックが「オン」設定されてチェック対象プロトコル名「P O P 3」、「S M T P」、「H T T P」が格納され、さらに、ジャンクメールチェックが「オン」設定されてチェック対象プロトコル名「P O P 3」が格納される。

【0 0 5 7】

このようなセキュリティ契約情報の格納処理が終了すると、契約代行サーバ3 4は、契約完了通知をP C 1 0に送信する（ステップS 9）。この契約完了通知には、セキュリティサーバ5 1のI Pアドレスと、セキュリティ契約情報に基づくチェック対象プロトコル名及び宛先ポート番号とが含まれている。

【0 0 5 8】

P C 1 0は上記契約完了通知を受信すると、受信した契約完了通知からセキュリティサーバ5 1のI Pアドレスと、チェック対象プロトコル名及び宛先ポート番号を抽出し、これらをルータ1 4に通知する（ステップS 1 0）。

【0 0 5 9】

これに応じて、ルータ1 4は、通知されたセキュリティサーバ5 1のI Pアドレスをフラッシュメモリ1 4 4に書き込むとともに、通知されたチェック対象プロトコルと宛先ポート番号とを関連付けたチェック対象プロトコルテーブルをフラッシュメモリ1 4 4に記憶させる（ステップS 1 1）。

【0 0 6 0】

さて、契約代行サーバ3 4は、ステップS 9の処理を行う一方で、セキュリティ契約情報をセキュリティサーバ5 1に送信する（ステップS 1 2）。

セキュリティサーバ5 1は、このセキュリティ契約情報を受信すると、受信したセキュリティ契約情報をセキュリティ契約情報D B 5 3に格納する（ステップS 1 3）。これにより、セキュリティチェックの契約に関する処理が終了することとなる。

【0 0 6 1】

（2）P O P 3を用いた受信メールに対するセキュリティチェック

次に、図17に示すシーケンスを参照しながら、POP3を用いた受信メールに対してセキュリティチェックを行う際の動作について説明する。

【0062】

まず、ユーザが例えばPC10を用いて受信メールの取得を指示する操作を行うと、PC10はこの操作を受け付け（ステップS21）、POPサーバ31に対する接続要求をパケットとして送信する（ステップS22）。そして、ルータ14は、この接続要求を受信する。

【0063】

ここで、ルータ14のCPU141は、図18に示す処理フローが記述されたルーティングプログラムを常時実行している（ステップS23）。

図18において、ルータ14のCPU141は、パケットを受信すると（ステップS101；Yes）、このパケットがチェック対象となるアプリケーション層プロトコルに従うパケットであるか否かを判断する（ステップS102）。より具体的には、CPU141は、パケットのTCPヘッダに含まれている宛先ポート番号と、フラッシュメモリ144のチェック対象プロトコルテーブル（図3参照）に記述されている宛先ポート番号とが一致する場合にはチェック対象であると判断し、一致しない場合にはチェック対象でないと判断する。ここでは、受信したパケットはPOP3に基づくものであるので、CPU141はチェック対象であると判断することになる（ステップS102；Yes）。

【0064】

次いで、CPU141は、IPヘッダに含まれる送信元アドレスがセキュリティサーバ51のIPアドレスであるか否かを判断する（ステップS103）。

ここで、IPヘッダに含まれている送信元アドレスを参照する理由は、セキュリティサーバ51から情報通信装置10～13宛に送信されたパケットがルータ14によってセキュリティサーバ51に返信されてしまうと、情報通信装置10～13にパケットが到達しなくなってしまうからである。また、上記理由に加えて、セキュリティサーバ51から送信されてきたデータであればコンピュータウィルス等の虞がないものと判断されるという理由もある。

ここでは、パケットの送信元アドレスはPC10のIPアドレスであるので、

セキュリティサーバ51のIPアドレスではないと判断する（ステップS103；No）。

【0065】

ステップS102及びステップS103における処理によって転送が必要と判断されると、CPU14は、セキュリティサーバ51と通信コネクションを確立しているか否かを判断する（ステップS104）。

ここで、通信コネクションが確立されていない場合は（ステップS104；No）、CPU14は、所定の接続手順に従ってセキュリティサーバ51との間で通信コネクションを確立する（ステップS105）。

【0066】

セキュリティサーバ51との間で通信コネクションが確立すると、図11で説明したように、CPU14は、宛先アドレスをセキュリティサーバ51のIPアドレスとし、送信元アドレスを自身のIPアドレスとし、さらにルータ14のシリアルナンバーを含むようにしてカプセル化を行う（ステップS106）。

【0067】

そして、CPU14は、カプセル化したパケットをセキュリティサーバ51に送信する（ステップS107）。

なお、ステップS102においてチェック対象プロトコルではないと判断された場合（ステップS102；No）と、ステップS103において送信元がセキュリティサーバ51であると判断された場合（ステップS103；Yes）には、CPU14は、パケットをカプセル化することなく、そのままルーティングすることになる。

このように、ルータ14がパケットを受信するたびに図18に示すフローが繰り返し実行されることになる。以下では、ルータ14が外部からパケットを受信する度に上記フローの説明を繰り返すことは省略するが、このフローは、（2）POP3を用いた受信メールに対するセキュリティチェック、だけでなく、（3）SMTPを用いた送信メールに対するセキュリティチェック、（4）HTTPレスポンスに対するセキュリティチェック、においても同様に実行される。

【0068】

再び、図17に戻り、システム全体の動作説明を行う。

図17のステップS23においては、ルータ14とセキュリティサーバ51との間で通信コネクションが確立されていない場合を示している。ステップS24～ステップS26は、図18のステップS105で説明した、ルータ14とセキュリティサーバ51との間で通信コネクションを確立する処理を示しており、以下簡単に説明する。

まず、ルータ14は、セキュリティサーバ51に対しコネクション確立要求を送信する（ステップS24）。このコネクション確立要求には、ルータ14のシリアルナンバーが含まれている。

【0069】

セキュリティサーバ51は接続要求を受信すると、このコネクション確立要求からシリアルナンバーを抽出し、シリアル情報DB52に記憶されているシリアルナンバーと照合してルータ14の正当性を確認する（ステップS25）。以下、この確認処理をルータ認証と呼ぶ。

【0070】

ルータ14の正当性が確認されると、セキュリティサーバ51は、ルータ14に許可応答を送信し、これによりルータ14とセキュリティサーバ51との間で通信コネクションが確立することになる（ステップS26）。

【0071】

次に、ルータ14は、図18のステップS106で説明したように、PC10から受信した接続要求を示すパケットをカプセル化してセキュリティサーバ51に送信する。これに応じて、セキュリティサーバ51は、図9で説明したように、ルータ認証を行い、さらに、受信したパケットに対して脱カプセル化を行った後、IPヘッダ内のIPアドレスを書き換え、書き換え後の接続要求をPOPサーバ31に送信する（ステップS27）。

【0072】

POPサーバ31は、接続要求を受信すると、これに応答して、PC10に対し認証情報の送信を要求する認証要求をパケットとして送信する（ステップS28）。この認証要求は、セキュリティサーバ51及びルータ14間でトンネリン

グされながら伝送され、PC10によって受信される。

【0073】

そして、PC10は、ユーザIDやパスワードといった認証情報をメモリから読み出し（ステップS29）、これをPOPサーバ31に送信する（ステップS30）。この際、これらの認証情報はステップS21の操作受付時にユーザによって入力されていてもよいし、PC10の不揮発性メモリから読み出されて自動送信されるような設定が予めなされていてもよい。

この認証情報は、ルータ14及びセキュリティサーバ51間でトンネリングやルータ認証が実行されながら伝送され、POPサーバ31によって受信される。

【0074】

POPサーバ31は認証情報を受信すると、この認証情報からユーザIDとパスワードを抽出し、ユーザ情報DB35に記憶されているユーザID及びパスワードと照合してユーザ認証を行う（ステップS31）。

これによりユーザの正当性が確認されると、POPサーバ31は、許可応答を送信する（ステップS32）。この許可応答は、セキュリティサーバ51及びルータ14間でトンネリングされながら伝送され、PC10によって受信される。

【0075】

PC10は、許可応答を受信すると、受信メールを要求するメール要求をPOPサーバ31に送信する（ステップS33）。このメール要求は、ルータ14及びセキュリティサーバ51間でトンネリングやルータ認証が実行されながら伝送され、POPサーバ31によって受信される。

【0076】

POPサーバ31はメール要求を受信すると、これに応答して、ユーザIDによって特定されるメールボックスから受信メールを示すメールデータを読み出し（ステップS34）、読み出したメールデータをパケットとしてPC10に送信する（ステップS35）。

【0077】

一方、セキュリティサーバ51は、ハードディスク装置515に記憶されているセキュリティチェックプログラムを常時実行しており、メールデータを受信す

ると、これに応じて、図6に示すセキュリティ契約情報DB532に記憶されている内容に従い、ウィルスチェック及びジャンクメールチェックを行う（ステップS36）。

ここで、セキュリティサーバ51によって受信されたデータがセキュリティチェックの対象となるメールデータであるか否かということは、受信したデータが電子メールの書式に従うものであるか否かということにより判断される。

【0078】

次いで、セキュリティサーバ51はセキュリティチェックを行った後のメールデータをパケットに分割してカプセル化を行い、PC10に送信する（ステップS37）。ルータ14は、このメールデータを脱カプセル化してPC10に送信する。

PC10は、メールデータを受信すると、POPサーバ31に対して切断要求を送信する（ステップS38）。これによって、PC10とPOPサーバ31との間の通信コネクションが切断され、処理が終了する。

なお、IMAP4を用いた受信メールに対するセキュリティチェックも、上述したPOP3の場合と同様の動作となる。

【0079】

（3）SMTPを用いた送信メールに対するセキュリティチェック

次に、図19に示すシーケンスを参照しながら、SMTPを用いた送信メールに対してセキュリティチェックを行う際の動作について説明する。

まず、ユーザがPC10を用いて電子メールの送信を指示する操作を行うと、PC10はこの操作を受け付け（ステップS51）、SMTPサーバ33に対する接続要求をパケットとして送信する（ステップS52）。

【0080】

ルータ14はこの接続要求を受信すると、図17のステップS24～S26において説明した動作と同様に、セキュリティサーバ51に対してコネクション確立要求を送信する（ステップS53）。このコネクション確立要求には、ルータ14のシリアルナンバーが含まれており、セキュリティサーバ51はこのシリアルナンバーを用いてルータ14の正当性を確認する（ステップS54）。これに

より正当性が確認されると、セキュリティサーバ51は、ルータ14に許可応答を送信し（ステップS55）、これにより通信コネクションが確立することになる。

【0081】

次に、ルータ14は、PC10から受信した接続要求を示すパケットをカプセル化してセキュリティサーバ51に送信する。これに応じて、セキュリティサーバ51は、ルータ認証を行い、さらに、受信したパケットに対して脱カプセル化を行った後、IPアドレスの書き換えを行い、書き換え後の接続要求をSMTPサーバ33に送信する（ステップS56）。

【0082】

SMTPサーバ33は、上記接続要求を受信すると、これに応じて、許可応答を送信する（ステップS57）。この許可応答は、セキュリティサーバ51及びルータ14間でトンネリングによって伝送され、PC10によって受信される。

【0083】

PC10は、許可応答を受信すると、送信メールを示すメールデータをパケットとしてSMTPサーバ33に送信する（ステップS58）。ルータ14は、PC10から受信したメールデータのパケットをカプセル化してセキュリティサーバ51に送信する。

セキュリティサーバ51は、このパケットを受信すると、これに応じてルータ認証を行い、さらに、受信したパケットに対して脱カプセル化を行う。そして、セキュリティサーバ51は、受信したパケットによって構成されるデータがSMTPに従うメールデータであることを検出すると、セキュリティ契約情報DB53に記憶されている内容に従ってウィルスチェックを行う（ステップS59）。

【0084】

次いで、セキュリティサーバ51はセキュリティチェックを行った後のメールデータをパケットに分割し、IPアドレスを書き換えてSMTPサーバ33に送信する（ステップS60）。

【0085】

SMTPサーバ33はメールデータを受信すると、PC10に対し受信通知を

送信し（ステップS 6 1）、これを受信したPC 1 0がSMTPサーバ3 3に対し切断要求を送信する（ステップS 6 2）。これによって、PC 1 0とSMTPサーバ3 3との間の通信コネクションが切断され、処理が終了する。

【0 0 8 6】

（4）HTTPを用いたコンテンツデータに対するセキュリティチェック

次に、図2 0に示すシーケンスを参照しながら、コンテンツデータに対してセキュリティチェックを行う際の動作について説明する。

まず、ユーザが例えばPC 1 0を用いてWWWサーバ6のURLを指定する等してコンテンツの取得を指示する操作を行うと、PC 1 0はこの操作を受け付け（ステップS 7 1）、WWWサーバ6に対するHTTPリクエストをパケットとして送信する（ステップS 7 2）。

【0 0 8 7】

ルータ1 4のCPU 1 4 1は、HTTPリクエストを受信すると、図1 7のステップS 2 4～S 2 6において説明した動作と同様に、セキュリティサーバ5 1に対してコネクション確立要求を送信する（ステップS 7 3）。このコネクション確立要求には、ルータ1 4のシリアルナンバーが含まれており、セキュリティサーバ5 1はこのシリアルナンバーを用いてルータ1 4の正当性を確認する（ステップS 7 4）。これによりルータ1 4の正当性が確認されると、セキュリティサーバ5 1は、ルータ1 4に許可応答を送信し（ステップS 7 5）、これにより通信コネクションが確立することになる。

【0 0 8 8】

次に、ルータ1 4は、PC 1 0から受信したHTTPリクエストをカプセル化してセキュリティサーバ5 1に送信する（ステップS 7 6）。

【0 0 8 9】

セキュリティサーバ5 1は、受信したパケットに対し脱カプセル化を行った後、IPヘッダのIPアドレスを書き換えてWWWサーバ6に送信する（ステップS 7 7）。

【0 0 9 0】

WWWサーバ6は、HTTPリクエストを受信すると、これに応答して、HT

TP リクエストに含まれるURLによって指定されるリソースからコンテンツデータを読み出し（ステップS 7 8）、読み出したコンテンツデータをHTTP レスポンスとしてPC 1 0に送信する（ステップS 7 9）。

【0 0 9 1】

セキュリティサーバ5 1はこのコンテンツデータを受信すると、セキュリティ契約情報DB 5 3に記憶されている内容に従ってウィルスチェックを行う（ステップS 8 0）。

次いで、セキュリティサーバ5 1は、セキュリティチェックを行った後のコンテンツデータをパケットに分割し、IP アドレスを書き換えてPC 1 0に送信する。ルータ1 4は、このHTTP レスポンスを脱カプセル化してPC 1 0に送信し、PC 1 0はこれを受信する（ステップS 8 1）。そして、PC 1 0は、受信したコンテンツデータを解釈してこれを表示する。

【0 0 9 2】

上述した実施形態によれば、ルータ1 4が受信したデータがPOP 3、IMAP 4 及びHTTP に従うデータである場合、ルータ1 4が上記データをセキュリティサーバ5 1に転送すると、セキュリティサーバ5 1は、受信したデータを当該データの宛先であるPOP サーバ3 1、IMAP サーバ3 2 又はWWW サーバ6 へ送信し、これに応答してPOP サーバ3 1、IMAP サーバ3 2 又はWWW サーバ6 から送信されてくるデータに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【0 0 9 3】

また、ルータ1 4が受信したデータがSMTP に従うデータである場合、ルータ1 4が受信したデータをセキュリティサーバ5 1に転送すると、これに応じて、セキュリティサーバ5 1が、ルータ1 4から転送されてきたデータに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【0 0 9 4】

さらに、上記のセキュリティチェックを行う場合、ユーザが所有する情報通信装置1 0～1 3 側ではなく、セキュリティサーバ5 1 側でセキュリティチェック

を行うので、ユーザがワクチンソフトをアップデートするというような作業が不要となる。これによりユーザの利便性を向上させることができる。

【0095】

さらに、ルータ14のシリアルナンバーを用いてルータ認証を行うので、セキュリティサーバ51は、不正なルータによるアクセスを排除することができる。

【0096】

さらに、セキュリティチェックの契約や課金に関する処理は、本来の処理主体であるべきセンタ5に代わってISP3が行うので、センタ5の管理者としては上記処理を行うための新たなシステムを開発する必要がない。また、ISP3側も、自身の既存システムに大きな変更を加えることなく、上記処理を実行できるので便利である。

【0097】

C：変形例

既述の通り、本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

【0098】

(1) ルータ14の形態

実施形態では、セキュリティサーバ51に対してデータを転送する装置としてルータ14を例示した。しかし、必ずしもこれに限定されるわけではなく、要は、情報通信装置10～13宛のデータや情報通信装置10～13から送信されるデータが伝送される伝送路に配置されて、上記データを中継するデータ中継装置であればよい。このようなデータ中継装置は、通常、その装置がサポートするプロトコル層に応じて、リピータ、ブリッジ、ルータ或いはゲートウェイというように異なる呼び方で呼ばれているが、実施形態で述べた構成及び動作を備えたデータ中継装置であれば、その呼び方に限定されることなく、本発明の技術思想に含まれる。

また、ルータ14はホームネットワーク1に利用されるだけでなく、例えばオフィス内に設置された社内LAN (Local Area Network) のような様々なローカルネットワークに利用可能である。

なお、ルータ 1 4 に接続される情報通信装置 1 0 ～ 1 3 は図 1 に示す 4 台に限定されず、もっと多くても少なくてもよいことはもちろんである。

【0 0 9 9】

(2) ルータ認証に用いる情報

実施形態では、ルータ認証を行う際に、そのルータ 1 4 の製造時に割り当てられたシリアルナンバーを用いていた。このシリアルナンバーは、ルータ 1 4 のハードウェアに対するシリアルナンバーであってもよいし、ルータ 1 4 に搭載されるルーティングプログラム等のソフトウェアに対するシリアルナンバーであってもよい。

また、ルータ認証に用いられる情報は、必ずしもシリアルナンバーに限定されるわけではない。要は、各ルータ 1 4 を識別できる情報であればよく、例えば、ルータ 1 4 に割り当てられた MAC アドレス等を代用してもよい。

また、ルータ 1 4 によって転送されるパケットに対してシリアルナンバーを記述する場合、その記述エリアは、カプセル化によって付加された TCP ペイロードに限定されるわけではなく、例えば、カプセル化によって付加された IP ヘッダや TCP ヘッダ等の適当なフィールドを利用すればよい。

【0 1 0 0】

(3) セキュリティチェックの対象となるプロトコル

実施形態では、POP 3、IMAP 4、SMTP、HTTP というプロトコルを例に挙げてセキュリティチェックを行うようにしていたが、必ずしもこれに限らず、例えば FTP (File Transfer Protocol) に従うデータに対してセキュリティチェックを行うようにしてもよい。

また、ルータ 1 4 が記憶しているチェック対象プロトコルテーブルには、チェック対象となるプロトコルが記述されていたが、これとは逆に、チェック対象ではないプロトコルを記述しておき、ルータ 1 4 はこのチェック対象プロトコルテーブルに記述されていないプロトコルに従うデータを受信した場合に当該データをセキュリティサーバ 5 1 に転送するようにしてもよい。

【0 1 0 1】

(4) ネットワーク構成

実施形態では、ホームネットワーク 1 と I S P 3 との間に介在するネットワークとして A D S L 網 2 を例示したが、これに限定されない。このネットワークの周波数帯域は広帯域であっても狭帯域であってもよく、例えば公衆電話網、I S D N (Integrated Service Digital NetWork) 網、C A T V (Cable TV) 網、いわゆる×D S L 網、携帯電話網等の公衆無線ネットワーク、衛星通信ネットワーク等の様々なネットワークが利用できる。

なお、このように図 1 とネットワーク形態が異なる場合には、A D S L モデム 1 5 に代えて、そのネットワークに適した変復調装置やプロトコル変換装置を用いる必要がある。

【0102】

(5) H T T P リクエストに対するセキュリティチェック

実施形態では、図 2 0 において説明したように、H T T P レスポンスとしてのコンテンツデータに対してセキュリティチェックを行うようになっていたが、H T T P リクエストに対してセキュリティチェックを行ってもよい。即ち、最近では、閲覧者に対し不適切なコンテンツを提供するサイトの存在も問題視されており、上述した H T T P リクエストに対するセキュリティチェックは、このようなサイトへの H T T P リクエストを排除することを目的としたものである。

具体的には、セキュリティサーバ 5 1 が、例えば成人向けのコンテンツを提供するサイトの URL を蓄積しておき、P C 1 0 からの H T T P リクエストを中継する際にはその H T T P リクエストに含まれる URL と、自身が蓄積している URL とを照合し、一致した場合には、その H T T P リクエストを廃棄すればよい。このようなセキュリティチェックを URL フィルタリングと呼ぶことにする。この URL フィルタリングを行うタイミングは、図 2 0 のステップ S 7 6 とステップ S 7 7 の間となる。

【0103】

(6) セキュリティチェック後の動作

実施形態において、セキュリティチェックサーバ 5 1 がセキュリティチェックを行ってコンピュータウィルスを駆除したり、ジャンクメールを廃棄したりした場合には、その旨を情報通信装置 1 0 ～ 1 3 に通知するようにすればさらに望ま

しい。

【0104】

(7) セキュリティ契約情報の配信

実施形態では、契約代行サーバ34がチェック対象プロトコル名と宛先ポート番号をPC10に送信すると、PC10がこれらをルータ14に転送するようになっていた。しかしこれに限定されず、契約代行サーバ34が直接、ルータ14に送信するようにしてもよい。

また、図15のステップS6において、契約時にPC10が送信したデータをルータ14が中継する際に、そのデータからチェック対象プロトコル名を抽出して、このチェック対象プロトコルに対応する宛先ポート番号と関連付けて記憶するようにしてもよい。

このようにすれば、処理のステップ数が削減されることになる。

【0105】

(8) プッシュ型配信への適用

実施形態では、情報通信装置10～13からのリクエストに応答してサーバから送信されてくる受信メールやコンテンツ、或いは、情報通信装置10～13から送信される送信メールに対してセキュリティチェックを行っていた。

しかしこれに限らず、インターネット4に接続されたサーバから情報通信装置10～13に強制的に配信してくるような場合（これをプッシュ型配信と呼ぶ）であっても本発明を適用することが可能である。この場合、ルータ14は、上記サーバから送信されてくる情報通信装置10～13宛のデータを受信すると、これをセキュリティサーバ51に転送する。一方、セキュリティサーバは、転送されてきたデータに対してセキュリティチェックを行った後に、そのデータの宛先である情報通信装置10～13に送信すればよい。

【0106】

(9) プログラムの形態

ルータ14やセキュリティサーバ51が上述した処理を行うために実行するプログラム（即ち、ルーティングプログラム、セキュリティチェックプログラム、契約申込画面配信プログラム及びプロキシプログラム）は、これらルータ14や

セキュリティサーバ51にアプリケーションプログラムとしてインストールされてもよいことはもちろんである。例えば、ルータ14、セキュリティサーバ51のCPU141、511を用いて読み取り可能な磁気記録媒体、光記録媒体あるいはROMなどの記録媒体に記録してこのプログラムを提供することができる。

また、このようなプログラムをインターネット4のようなネットワーク経由でルータ14やセキュリティサーバ51にダウンロードさせることももちろん可能である。

なお、製造後のルータ14にルーティングプログラムをインストールする際には、このルーティングプログラムは、ROM142ではなく、フラッシュメモリ144に記憶されることになる。

【0107】

【発明の効果】

上述したように本発明によれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【0108】

また、本発明によれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【0109】

【図面の簡単な説明】

【図1】 本発明の実施形態に係るシステム全体の構成を示すブロック図である。

【図2】 実施形態におけるルータの構成を示すブロック図である。

【図3】 実施形態におけるチェック対象プロトコルテーブルに記述されているデータの一例を示すフォーマット図である。

【図4】 実施形態におけるセキュリティサーバの構成を示すブロック図で

ある。

【図 5】 実施形態におけるシリアル情報DBに記憶されているシリアル情報の一例を示すフォーマット図である。

【図 6】 実施形態におけるセキュリティ契約情報DBに記憶されているセキュリティ契約情報の一例を示すフォーマット図である。

【図 7】 実施形態におけるユーザ情報DBに記憶されているユーザ情報の一例を示すフォーマット図である。

【図 8】 実施形態における課金情報DBに記憶されている課金情報の一例を示すフォーマット図である。

【図 9】 実施形態におけるデータ中継の仕組みを説明する説明図である。

【図 10】 実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図 11】 実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図 12】 実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図 13】 実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図 14】 実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

である。

【図 15】 実施形態において契約申込みを行う際のシステム全体の動作を示すシーケンス図である。

【図 16】 実施形態における契約申込画面の一例を示す模式図である。

【図 17】 実施形態において受信メールに対してセキュリティチェックを行う際のシステム全体の動作を示すシーケンス図である。

【図 18】 実施形態におけるルータのCPUがセキュリティチェックプログラムを実行する際のフローチャートである。

【図 19】 実施形態において送信メールに対してセキュリティチェックを

行う際のシステム全体の動作を示すシーケンス図である。

【図20】 実施形態においてコンテンツデータに対してセキュリティチェックを行う際のシステム全体の動作を示すシーケンス図である。

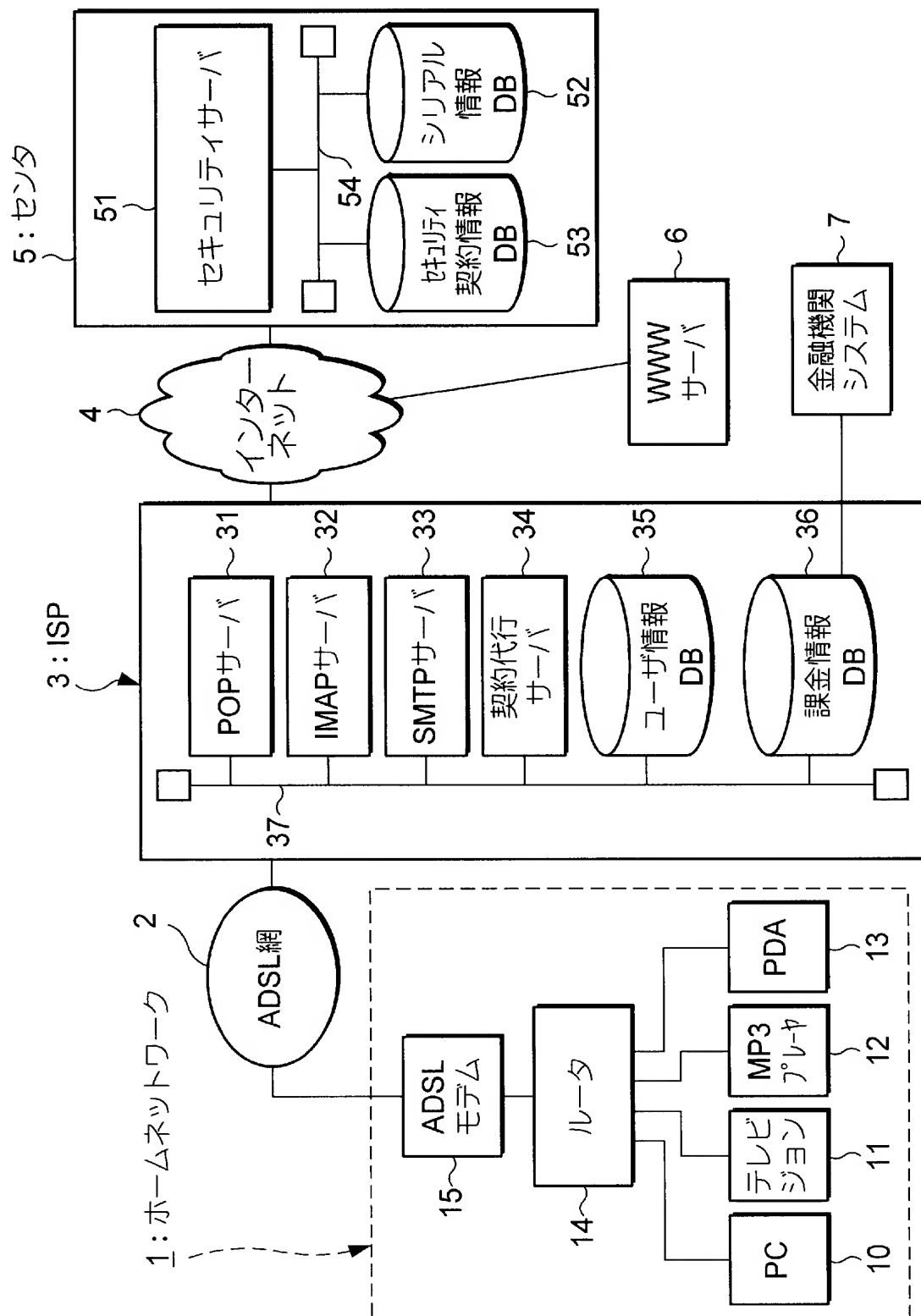
【符号の説明】

1・・・ホームネットワーク、2・・・ADSL網、
3・・・ISP（プロバイダ）、31・・・POPサーバ（宛先）、
32・・・IMAPサーバ（宛先）、33・・・SMTPサーバ（宛先）、
34・・・契約代行サーバ（プロバイダの通信装置）、
35・・・ユーザ情報DB（記憶手段）、36・・・課金情報DB（課金手段）、
4・・・インターネット、5・・・センタ、
51・・・セキュリティサーバ（サーバ、転送先）、
511・・・CPU（データ受信手段、データ送信手段、応答データ受信手段、セキュリティチェック手段、応答データ送信手段、認証手段）、
512・・・ROM、513・・・RAM、
514・・・通信部（データ受信手段、データ送信手段、応答データ受信手段、応答データ送信手段）、
515・・・ハードディスク装置、52・・・セキュリティ契約情報DB、
53・・・シリアル情報DB（記憶手段）、6・・・WWWサーバ（宛先）、
7・・・金融機関システム、10・・・PC（情報通信装置）、
11・・・テレビジョン（情報通信装置）、
12・・・MP3プレーヤ（情報通信装置）、
13・・・PDA（情報通信装置）、14・・・ルータ（データ中継装置）、
141・・・CPU（転送手段、通信手段、判断手段、アドレス受信手段、決定手段、要否判断情報受信手段）、
142・・・ROM（記憶手段）、143・・・RAM、
144・・・フラッシュメモリ（アドレス記憶手段、要否判断情報記憶手段）、
145・・・表示部、146・・・LAN通信部（通信手段）、
147・・・WAN通信部（通信手段、転送手段、アドレス受信手段、要否判断

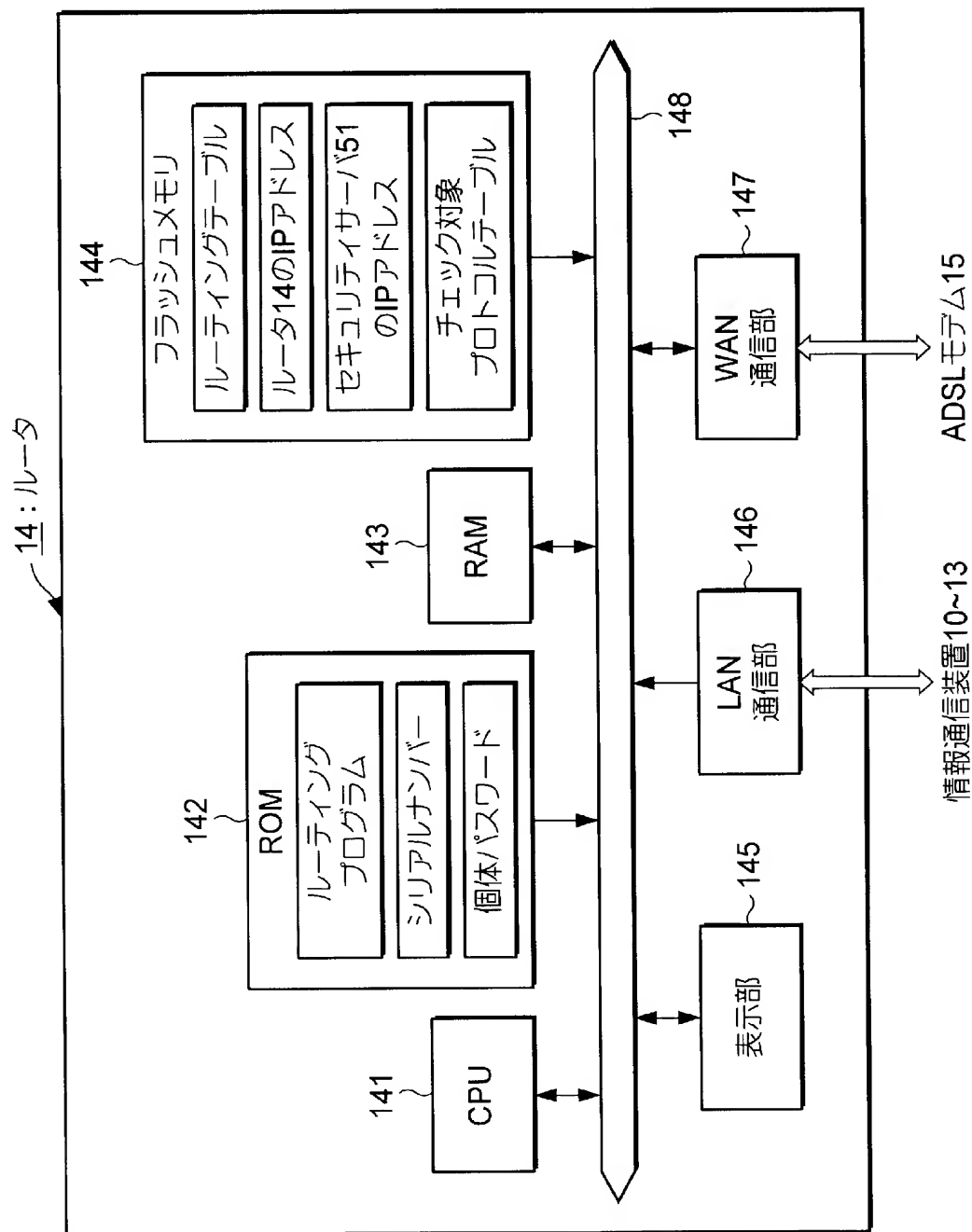
情報受信手段)、15・・・ADSLモデム。

【書類名】 図面

【図 1】



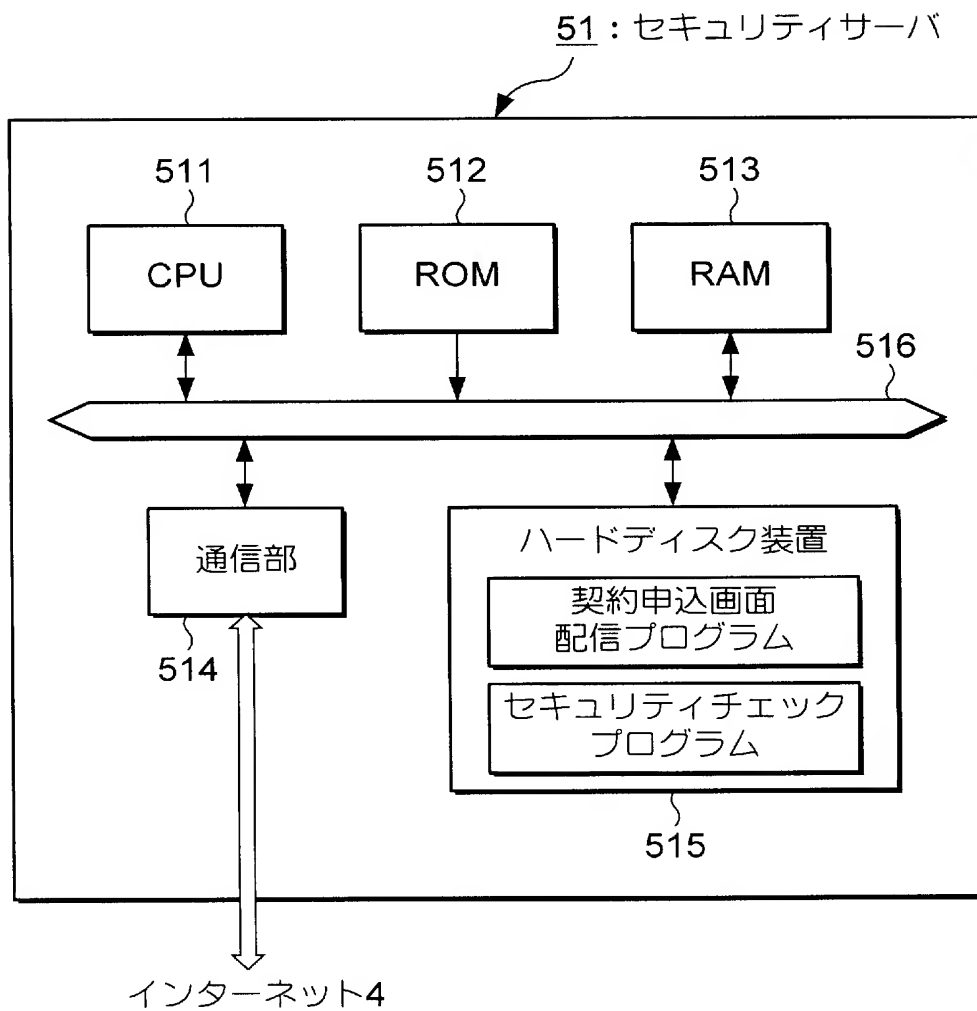
【図2】



【図3】

チェック対象プロトコル	宛先ポート番号
POP3	110
SMTP	25
HTTP	80

【図4】



【図 5】

シリアルナンバー	個体パスワード
S000001	abc123
S000002	syt254
S000003	ztc921
⋮	⋮
S018110	hfn377

【図6】

シリアルナンバー	S000001	S000002
セキュリティチェック の内容			
ウイルスチェック	オン	オフ
チェック 対象 プロトコル	POP3	—
	SMTP	—
	HTTP	—
	—	—
ジャンクメール チェック	オン	オン
チェック 対象 プロトコル	POP3	IMAP4
	—	—

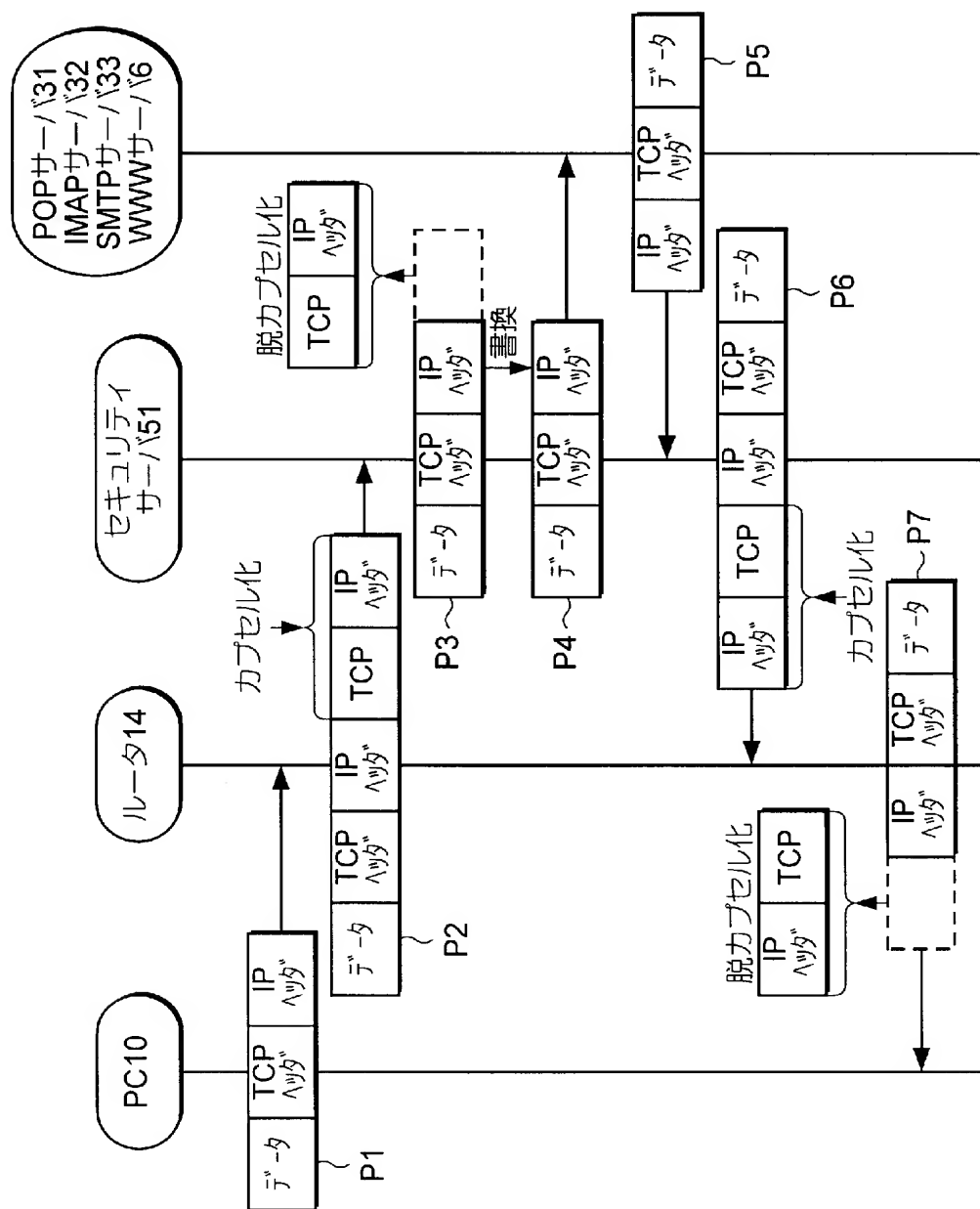
【図 7】

ユーザーID	aaa	bbb
パスワード	xxxxzz	kkkttt
シリアルナンバー	S000001	—
個体/パスワード	abc123	—
セキュリティチェック の内容			
ウイルスチェック	オン	—
チェック 対象 プロトコル	POP3	—
	SMTP	—
	HTTP	—
	—	—
ジャンクメール チェック	オン	—
チェック 対象 プロトコル	POP3	—
	—	—
ユーザー名前
住 所
生年月日
.	.	.	.
.	.	.	.
.	.	.	.

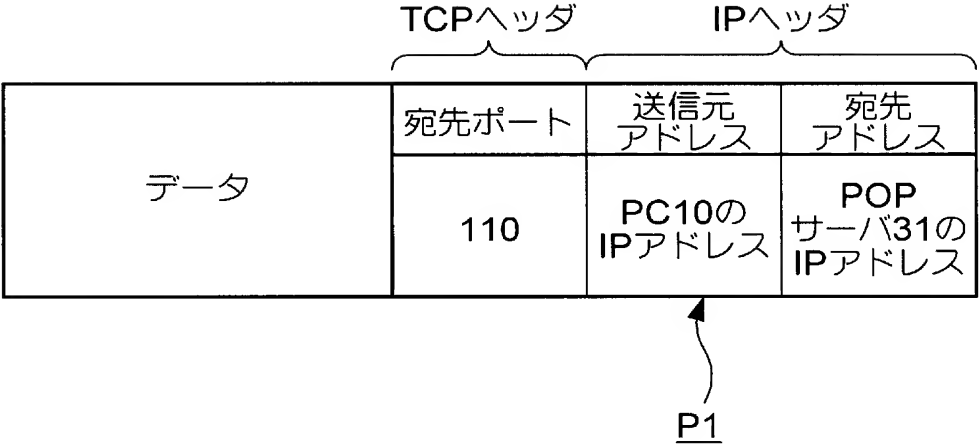
【図 8】

ユーザID	aaa	bbb
銀行口座	〇〇銀行 △△支店 □座番号:XXXXXX	××銀行 □□支店 □座番号:XXXXXX
ISP課金額	5000	3000
セキュリティ チェック課金額	3000	—
ウイルス チェック 課金額 ジャクメール チェック 課金額	2000	—
	1000	—
課金額合計	8000	3000

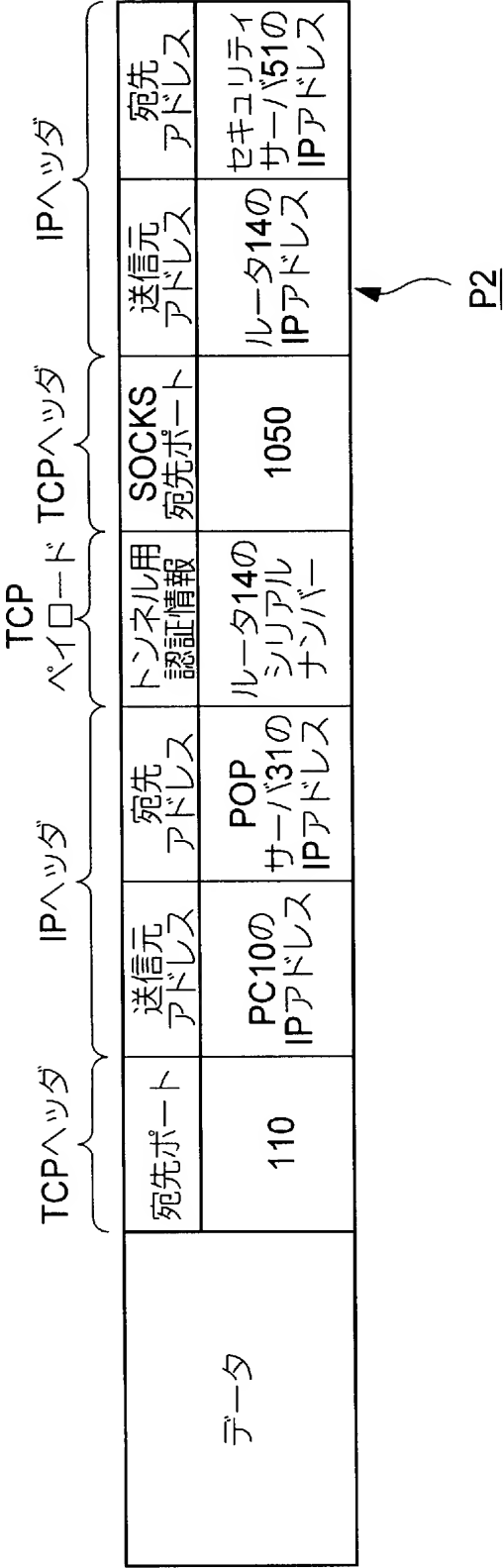
【図9】



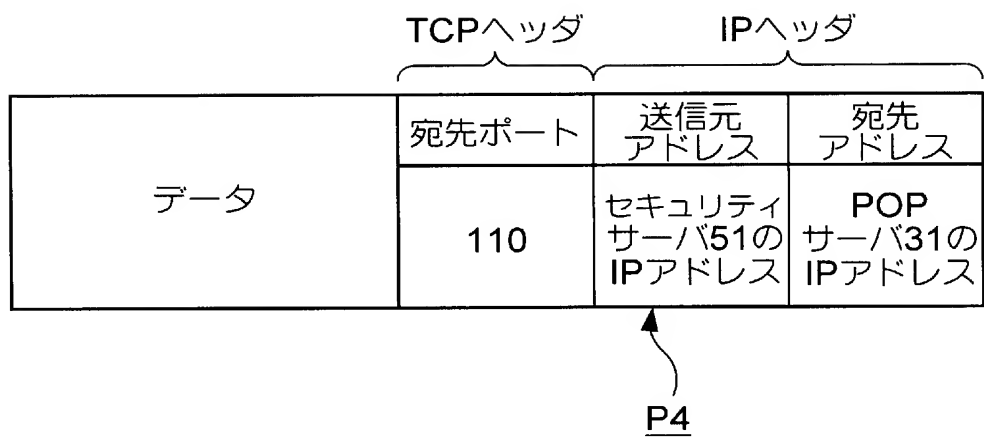
【図 1 0】



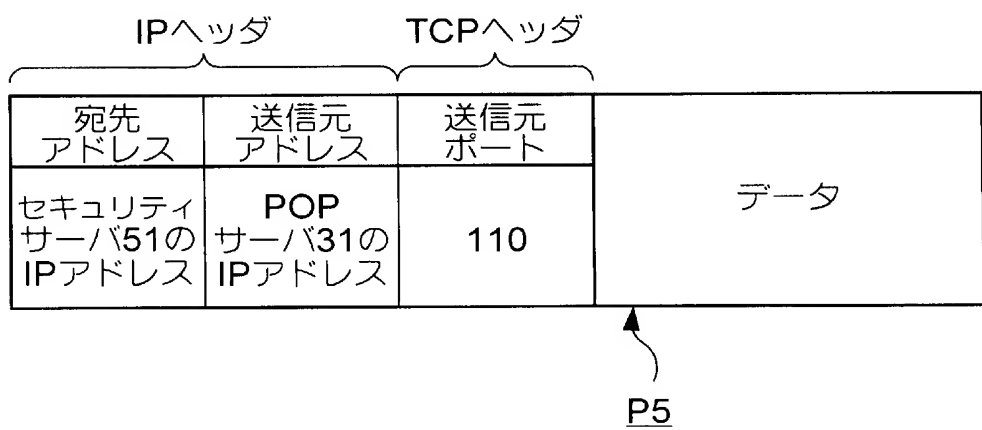
【図 1 1】



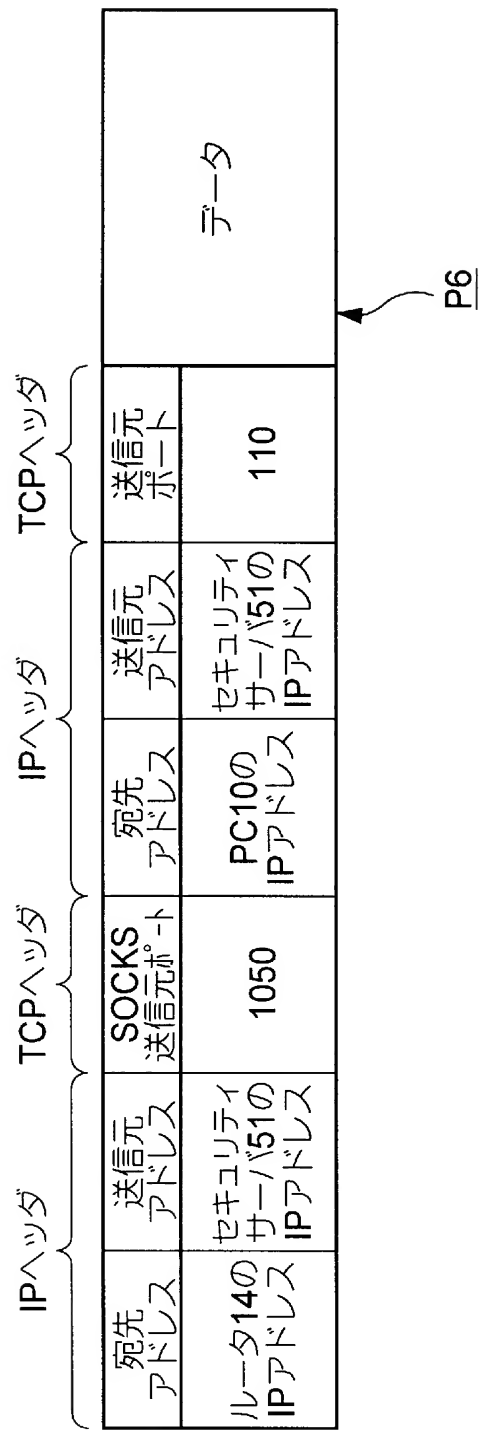
【図12】



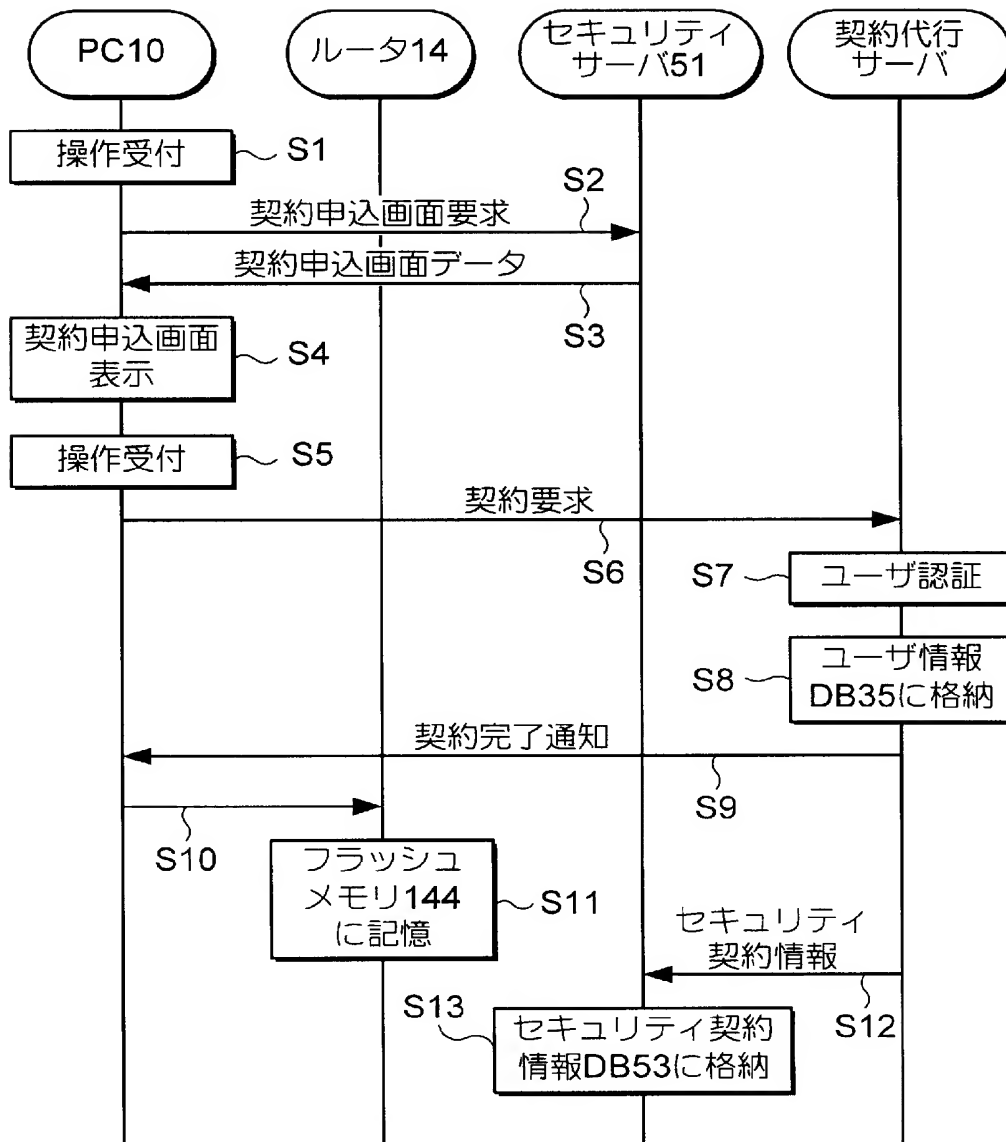
【図13】



【図 1 4】



【図15】



【図16】

契約のお申し込み

ISP名 MB F1

シリアルナンバー F2

個体パスワード F3

ユーザーID F4

パスワード F5

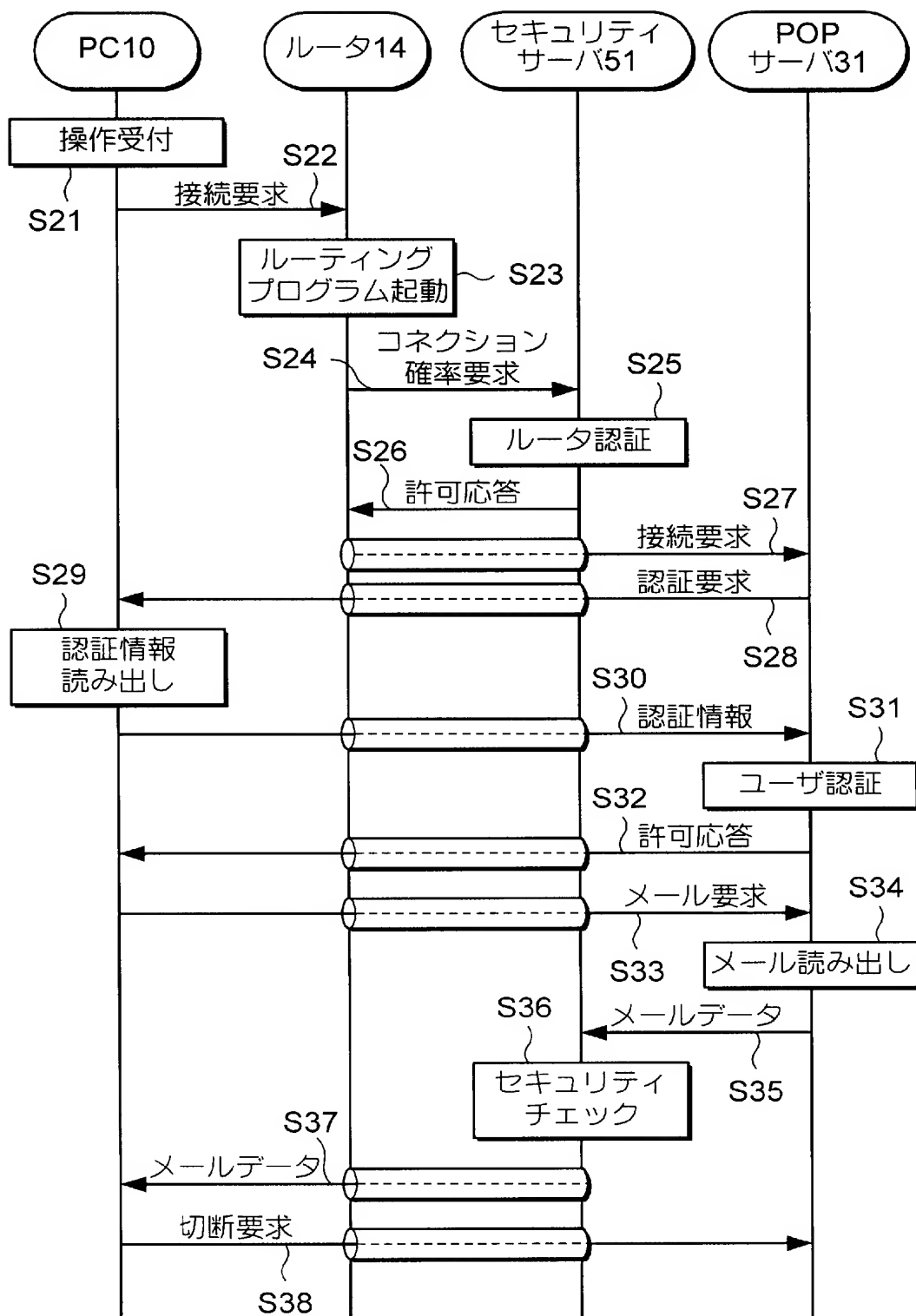
セキュリティチェック ウィルスチェック ☒ F6
(□の中に✓ POP3 ☒ F7
して下さい) IMAP4 ☒ F8
SMTP ☒ F9

ジャンクメールチェック ☒ F10

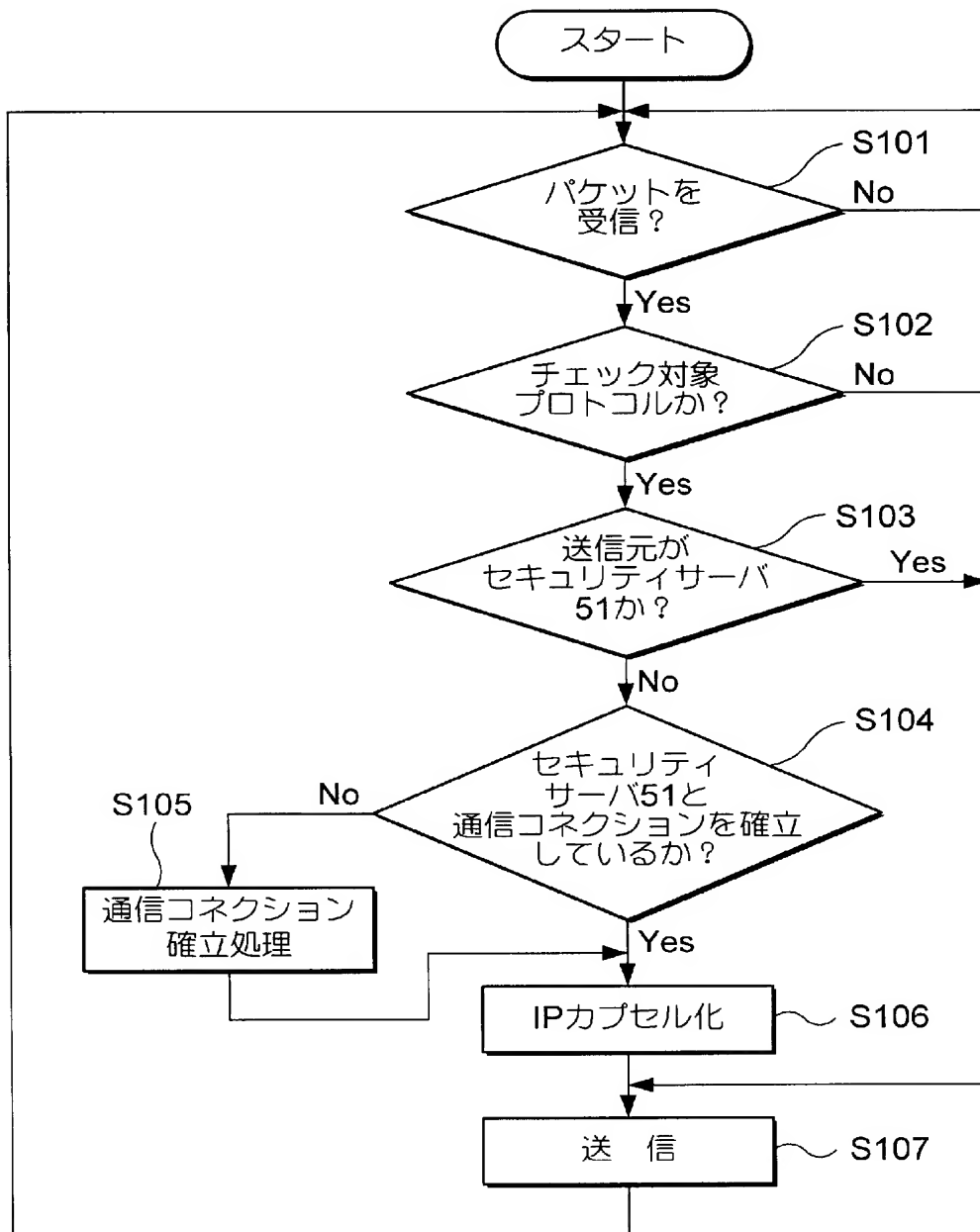
POP3 ☒ F11 IMAP4 ☐ F12

SB

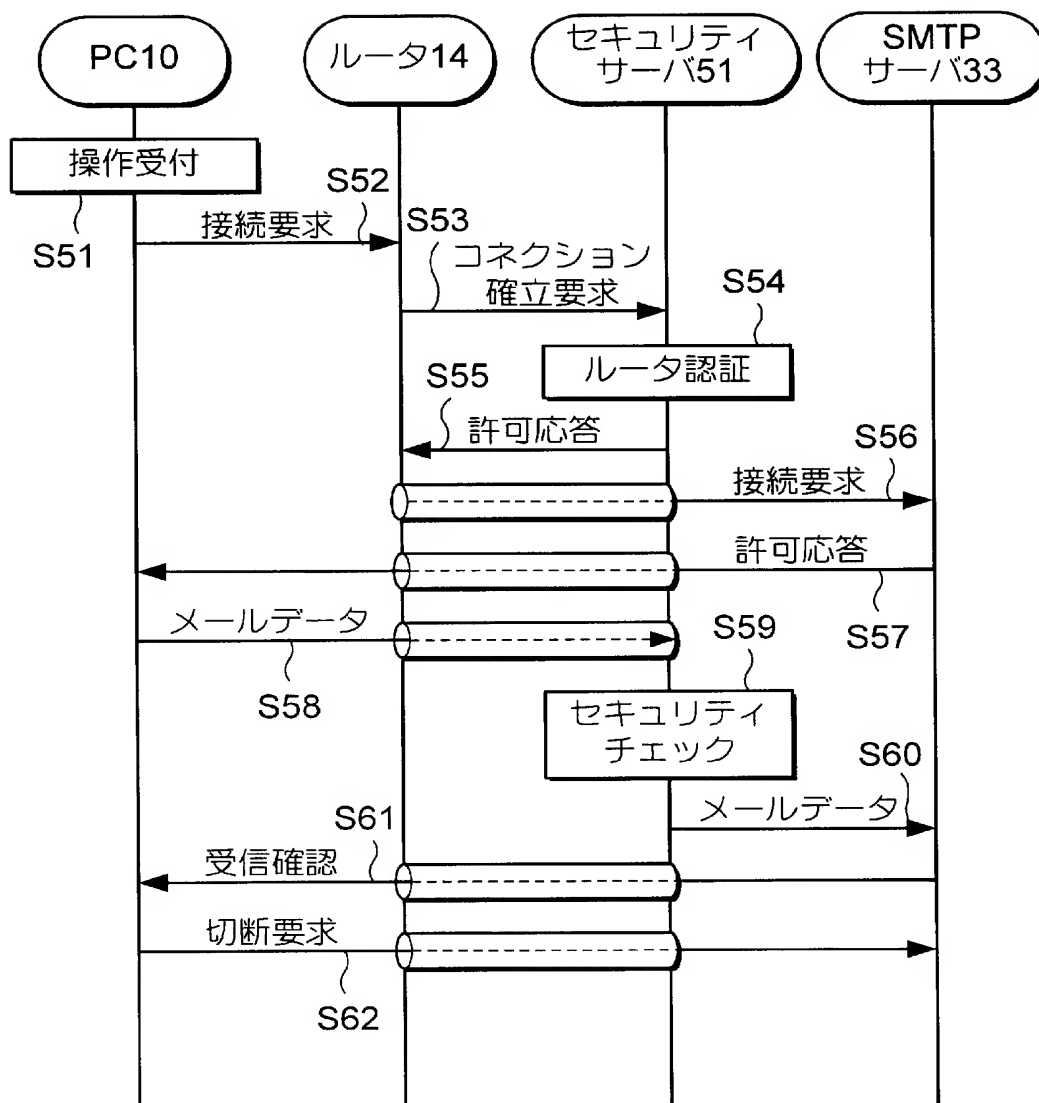
【図17】



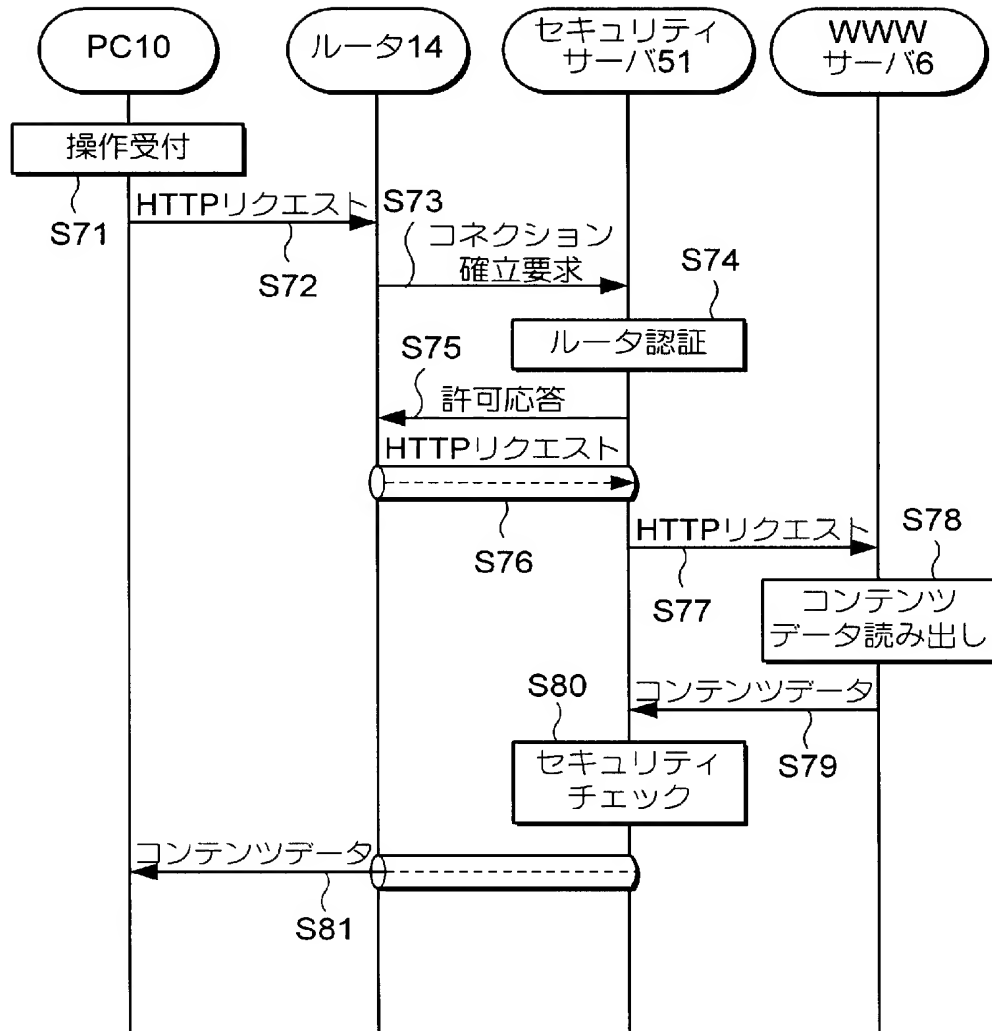
【図18】



【図19】



【図20】



【書類名】 要約書

【要約】

【課題】 インターネット等のコンピュータネットワークにおいて、コンピュータウィルスやジャンクメール等の様々な不正行為による被害を防止する。

【解決手段】 ルータ 1 4 は、情報通信装置 1 0 ～ 1 3 から受信したデータをセンタ 5 のセキュリティサーバ 5 1 に転送する。センタ 5 では、受信したデータに対してコンピュータウィルスの有無等进行检查し、チェック後のデータをそのデータの宛先へ送信する。

【選択図】 図 1

【書類名】 手続補正書

【提出日】 平成14年 2月27日

【あて先】 特許庁長官 殿

【事件の表示】

【出願番号】 特願2001-165580

【補正をする者】

【識別番号】 397011166

【氏名又は名称】 トレンドマイクロ株式会社

【代理人】

【識別番号】 100098084

【弁理士】

【氏名又は名称】 川▲崎▼ 研二

【電話番号】 03-3242-5481

【手続補正 1】

【補正対象書類名】 特許願

【補正対象項目名】 発明者

【補正方法】 変更

【補正の内容】

【発明者】

【住所又は居所】 アール．オー．シー，台湾，台北，チュン フォア，エス．アールディー．エスイーシー．2，319，9階 トレンドマイクロインコーポレイテッド内

【氏名】 リー，フランク

【発明者】

【住所又は居所】 アメリカ合衆国，95129，カリフォルニア，サンノゼ，ダートムア ウェイ，6543

【氏名】 リャン，ジェレミー ジー

【発明者】

【住所又は居所】 アメリカ合衆国，91107，カリフォルニア，パサデナ，

エルカンポ ドライブ, 9 6 5

【氏名】 チェン, エバ

【発明者】

【住所又は居所】 アール. オー. シー, 台湾, 台北, 1 0 4, ジャンシャン
チュウ, ジャングウオ エヌ ロード, セクション1, レーン1 2 4, ナンバ
ー3, 5階

【氏名】 リン, イジン

【提出物件の目録】

【物件名】 宣誓書 1

【物件名】 理由書 1

(B)20200390128



宣 告 書

平成14年 2 月 12 日

発明者

住所 アール・オー・シー、台湾、台北、チュン フォア、エス・
アールディー・エスイーシー、2, 319, 9階
トレンドマイクロ インコーポレイテッド

氏名 リー, フランク

住所 アメリカ合衆国, 95129, カリフォルニア, サンノゼ,
ダートムア ウェイ, 6543

氏名 リャン, ジェレミー ジー

住所 アメリカ合衆国, 91107, カリフォルニア, バサデナ,
エルカンボ ドライブ, 965

氏名 チェン, エバ

住所 アール・オー・シー、台湾、台北、104,
ジャンシャン チュウ, ジャングウオ エヌ ロード,
セクション1, レーン124, ナンバー3, 5階

氏名 リン, イジン

下記発明は、私共4名の共同発明であることに相違ありません。

記

1. 出願番号

特願2001-165580

2. 発明の名称

データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

(B)20200390128


理 由 書

1. 事件の表示

特願 2001-165580

2. 発明の名称

データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

本件は、発明者4名で出願すべきところ、発明者「リャン、ジェレミー ジー」「チェン、エバ」「リン、イジン」を記載し忘れて出願してしまいました。

この誤記に至ったのは、代理人の不注意によるものであります。つきましては、上記発明者を追加致したく、必要書類を添えて提出致しますので、手続き方、宜しくお願い申し上げます。

以 上

平成14年2月27日

出 願 人 代 理 人
弁 理 士 川 崎 研 二



出願人履歴

397011166

19980603

住所変更

東京都渋谷区代々木2丁目2番1号 小田急サザンタワー10階
トレンドマイクロ株式会社

397011166

20031126

住所変更

東京都渋谷区代々木2-1-1 新宿マインズタワー
トレンドマイクロ株式会社